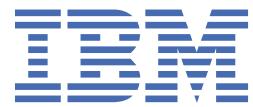


IBM OpenPages with Watson
Version 9.0.0

Administrator's Guide



Note

Before using this information and the product it supports, read the information in “[Notices](#)” on page [967](#).

Product Information

This document applies to IBM OpenPages with Watson 9.0.0 and may also apply to subsequent releases.

Licensed Materials - Property of IBM Corporation.

© Copyright IBM Corporation, 2003, 2023.

US Government Users Restricted Rights – Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

© Copyright International Business Machines Corporation .

US Government Users Restricted Rights – Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

Contents

Introduction.....	xxi
Chapter 1. IBM OpenPages with Watson.....	1
How IBM OpenPages with Watson can help.....	1
Installation locations (on prem).....	2
Special characters in passwords.....	5
Variables and placeholders.....	6
Chapter 2. What's new?.....	9
Version 9.0.0.0.....	9
Version 8.3.0.2.....	12
Version 8.3.0.1.....	13
Version 8.3.0.0.....	14
Version 8.2.0.4.....	19
Version 8.2.0.3.....	20
Version 8.2.0.2.....	22
Version 8.2.0.1.....	24
Version 8.2.0.0.....	27
Chapter 3. OpenPages for Cloud Pak for Data.....	33
Documentation for IBM OpenPages for IBM Cloud Pak for Data administrators.....	33
Chapter 4. System Admin Mode (SAM).....	37
Enabling and disabling System Admin Mode.....	37
Chapter 5. Users, groups, and domains.....	39
The OPAdministrators group.....	39
Planning user administration.....	40
The Super Administrator.....	41
Creating a Super Administrator.....	42
Delegate administrator permissions.....	42
Types of administrator permissions.....	43
Assigning, modifying, and removing administrator permissions on groups.....	45
LDAP and user provisioning.....	46
Importing an LDAP certificate to the local truststore	46
Configuring LDAP access for user provisioning	47
Provisioning users.....	47
Creating user accounts	48
Modifying user accounts.....	49
Copying access from one user to another.....	50
Creating an organizational group	51
Associating and disassociating a group	51
Defining application permissions.....	51
Setting group application permissions.....	52
Types of application permissions.....	52
Application permissions not contained under the SOX heading.....	58
Configure password requirements.....	60
Configuring password policies.....	60
Updating the password encryption algorithm.....	61

Chapter 6. Security.....	67
Role-based security model.....	67
Security context points.....	69
Extending security context points.....	70
Security domains.....	72
Moving business entities.....	73
Copying business entities.....	73
Role-based access control permissions.....	73
Role templates.....	75
Accessing Role Templates.....	75
Adding a role template	76
Modifying a role template.....	77
Enabling and disabling a role template.....	77
Deleting a role template.....	77
Assigning and revoking roles.....	78
Assigning and removing a role from a user or group	78
Viewing roles assigned to users or groups.....	79
Security rules.....	80
Record level security.....	81
Field level security.....	92
Paths for parent and child objects.....	95
Terms for data types.....	96
Grammar for security rules.....	98
Enabling or disabling a security rule.....	101
Validating a formula for a security rule.....	102
Deleting a security rule.....	102
Best practices for security rules.....	102
Encryption.....	104
Create a keystore.....	105
Configure a custom encryption key for passwords in properties files.....	106
Configure field level encryption.....	110
Updating the encryption keystore.....	111
LDAP user authentication.....	113
Configuring the LDAP Authentication Module.....	113
Setting up mixed-mode authentication.....	115
Configuring a multi-forested LDAP authentication.....	116
Chapter 7. Managing the reporting schema	117
Changes that require the reporting schema to be updated or re-created.....	117
Populating past reporting periods.....	119
Reporting schema permissions.....	119
Creating or re-creating the reporting schema	120
Updating the reporting schema.....	121
Generating the reporting schema and framework from a command line.....	121
Chapter 8. Managing reports.....	125
Platform reports.....	125
Running reports from a dashboard.....	129
Adding reports to OpenPages.....	129
Method 1: Manually add and edit pages to create and modify reports.....	130
Understanding reports.....	130
Locating report files.....	130
Accessing report pages and page templates.....	131
Manually creating an instance of a report.....	131
Manually creating an instance of a Cognos dashboard or story	135
Method 2: Automatically publishing Cognos reports.....	138

Report publishing limitations	139
Publishing a report.....	139
Modifying the displayed report name or description.....	139
Creating an interactive JSP report	139
Running an interactive JSP report.....	140
Restricting access to reports	141
Setting permissions on JSPs and reports.....	141
Securing access to the report portal.....	142
Chapter 9. System file management.....	145
Managing system files and folders	148
System file modification.....	149
Adding and modifying system files	150
Refreshing trigger configurations.....	151
Chapter 10. Fields and field groups.....	153
Definition of fields.....	153
Definition of a field group.....	153
Requirements for new fields.....	153
Field naming guidelines	154
Data types.....	155
Colors for field value ranges.....	158
Supported color palettes for field values.....	159
Defining field groups.....	160
Adding existing field groups to object types.....	160
Defining fields and adding them to field groups.....	161
Making fields required or optional.....	162
Encrypting field values.....	163
Decrypting field values.....	164
Setting a default value for an object field.....	164
Defining Boolean fields	164
Defining business entity selector fields	165
Defining a classifier field.....	165
Defining currency fields.....	166
Modifying currency exchange rates.....	167
Defining a date field	169
Defining decimal fields.....	169
Defining enumerated string fields.....	170
Defining integer fields.....	171
Defining long string fields.....	172
Defining simple string fields.....	172
Defining user/group fields.....	173
Changing the display type for users and groups.....	175
Configuring reporting fragment fields.....	176
Overall configuration for reporting fragment fields.....	177
Planning considerations for reporting fragment fields.....	177
Defining a reporting fragment field.....	178
Obtaining information from Cognos.....	179
Creating computed fields	181
Modeling a new computed field.....	182
Defining a computed field.....	183
Using computed fields with multiple namespaces.....	185
Nesting computed fields.....	185
Troubleshooting: Computed fields validation.....	186
Troubleshooting: Computed field equation length limitation.....	186
Troubleshooting: Computed fields with cross products.....	186
Troubleshooting: Optimizing report request performance.....	187

Troubleshooting: Computed field query direction performance.....	188
Using object fields to launch JavaServer Pages and external URLs.....	188
Attributes in the URL configuration string.....	189
URL configuration string examples.....	191
Configuring application text.....	192
Adding a URL launcher field	193
Adding a URL launcher field to profiles and views.....	193
Running the Schema Analysis report.....	193
Chapter 11. Object types.....	195
Platform object types.....	195
Solution schema visualizations	195
Using the solution schema visualization editor	196
Creating a solution schema visualization	197
Accessing object types.....	198
Working with object types	198
Editing object type properties.....	199
Disabling associations between object types.....	200
Enabling associations between object types.....	200
Configuring OpenPages to associate a large number of child objects.....	201
Limiting parent and child relationships.....	202
Configuring file types for file attachments	202
Adding a file type.....	203
Enabling and disabling file types.....	203
Enabling and disabling global search for file types.....	204
Configuring filters for an object type.....	204
Filter considerations.....	205
Limitations on special characters in filters for long string fields.....	205
Adding filters to object types.....	208
Configuring dependent fields	211
Adding and working with dependent fields	212
Configuration settings for creating new objects	213
Controlling the availability of object types with the New button on Grid Views.....	213
Configuring dependent picklists.....	214
Adding and working with dependent picklists	214
Excluding fields from a subsystem.....	216
Selecting the fields to exclude.....	216
Changing the subsystem for an excluded field.....	217
Removing excluded fields.....	218
Chapter 12. Profiles.....	219
Guidelines for working with profiles.....	219
Accessing profiles.....	220
Creating a profile	220
Setting default and fallback profiles.....	221
Editing a profile.....	222
Deleting a profile.....	222
Enabling a profile.....	222
Disabling a profile.....	223
Associating profiles to a user.....	223
Associating users to a profile.....	224
Associating groups to a profile.....	224
Disassociating users from a profile.....	225
Disassociating groups from a profile.....	225
Including object types in a profile.....	226
Removing object types from a profile.....	226
Adding reports to a profile.....	227

Including fields in an object type.....	227
Excluding fields from an object type.....	228
Setting a field in a profile to required or optional.....	228
Chapter 13. Configuring the UI.....	229
Setting up the UI.....	229
Home page, dashboard, and tabs.....	230
Defining a dashboard for a profile.....	231
Adding a Search panel.....	232
Customizing the Primary menu.....	233
Changing the order of menu items.....	233
Adding object types to a submenu.....	235
Creating a new top-level menu item.....	236
Creating tags.....	237
Integrating WalkMe.....	238
Configuring a Net Promoter Score survey.....	239
Exporting and importing dashboards	241
Themes.....	241
Defining custom themes.....	243
Chapter 14. Views.....	247
Grid Views.....	249
Creation Views.....	250
Task Views.....	251
Admin Views.....	252
Associating objects by using Admin View.....	254
Creating custom views.....	255
Creating a custom view from a system view.....	255
Creating custom Grid Views.....	255
Creating custom Creation Views.....	260
Creating custom Task Views.....	265
Creating custom Admin Views.....	271
View Designer.....	272
Displaying debug information.....	277
Editing JSON for a view definition.....	277
Adding general elements to a view.....	278
Adding and configuring fields on views.....	287
Adding and configuring relationship fields on views.....	290
Adding actions to relationship fields.....	313
Configuring rules.....	318
Chapter 15. Configuring GRC Calculations.....	327
Setting up GRC Calculations.....	327
Calculation fundamentals.....	328
GRC Calculations FAQs.....	330
Designing a calculation.....	333
Common calculation use cases	336
Managing calculation definitions.....	337
Defining a calculation.....	338
Expressions in GRC Calculations.....	342
Syntax rules for expressions.....	344
Tutorial: writing expressions.....	347
Working with lists.....	349
Object fields	351
System variables	352
Functions for string values	353
Functions for lists and numerical values.....	354

Functions for dates.....	357
Functions for currency values.....	359
If/then/else/endif statements.....	360
Running a calculation as an administrator.....	364
Testing and debugging a calculation.....	365
Customizing email notifications for GRC Calculations.....	366
Chapter 16. Configuring GRC Workflow	369
Setting up GRC Workflow.....	369
GRG Workflow fundamentals.....	370
Workflow definitions and workflow instances.....	370
How workflows are started.....	371
Types of users who interact with workflows	372
How users interact with workflows	373
System workflow fields.....	376
Using variables, functions, and fields	377
Interpreting and viewing due dates.....	379
Designing a workflow.....	379
Using the GRC Workflow Designer.....	382
Workflow list.....	383
GRG Workflow Designer components	383
Using the keyboard in the GRC Workflow Designer.....	385
Defining a workflow.....	391
Defining workflow properties	392
Workflow stages.....	397
Defining a start stage.....	397
Defining a standard stage.....	397
Defining an end stage.....	402
Deleting stages.....	405
Workflow actions.....	405
Defining a workflow action.....	407
Defining a workflow action that creates objects.....	413
Defining a workflow action that runs a custom action	415
Defining a workflow action that locks or unlocks objects.....	417
Defining a workflow action that sets fields.....	420
Defining a workflow action that starts a workflow.....	422
Defining a workflow action that runs a calculation.....	425
Deleting actions.....	427
Customizing email notification templates in workflows.....	427
Creating objects based on scores in a questionnaire assessment.....	429
Starting workflow instances in bulk.....	430
Managing workflow instances.....	431
Exporting and importing workflow definitions.....	432
Customizing email notifications for GRC Workflow	432
Reporting on information in workflow instances.....	434
Chapter 17. Scheduler.....	435
Managing jobs	435
Defining a custom job.....	437
Defining a job that runs a JSP report.....	438
Implementing a Java class for custom jobs	440
Chapter 18. Localizing text.....	443
Configuring client systems to display Asian characters.....	443
Language and locale support.....	444
Localizing object text.....	445
Modifying object text	445

Localizing system fields.....	447
Localizing application text.....	447
Modifying application text	449
Modifying the bucket heading format of the phonebook.....	449
Modifying how the names of users are displayed.....	450
Defining messages and behavior on the login screens.....	451
The Custom folder.....	455
Adding new keys.....	455

Chapter 19. Reporting periods, object resets, and rulesets.....457

Reporting period interactions.....	457
Using System Admin Mode with reporting periods	458
Reporting period permissions and settings.....	458
Creating a finalized a reporting period	458
Disabling finalized reporting periods.....	459
Deleting a reporting period	459
Object resets.....	460
Creating a ruleset.....	461
Sample ruleset.....	461
Ruleset tag library.....	463
Loading the ruleset.....	468
Performing the object reset.....	468
Starting the object reset	469
Refreshing the reporting database after the reset.....	471
Exporting rulesets to an XML file.....	471

Chapter 20. Viewing the Configuration and Settings page.....473

Managing settings	473
Paths for settings in data loader files.....	474
Applications folder settings.....	474
Configure the browser cache.....	475
Displaying the accessibility link.....	475
Defining the Privacy and Acceptable Use menu items.....	476
Display or hide field guidance.....	477
Display or hide system generated field guidance.....	478
Disable the New capability from various launch points.....	478
Modify the deletion interval for a reporting period.....	479
Show hidden settings.....	479
Specify the browsers that can access IBM OpenPages.....	479
User provisioning settings.....	480
Actor selectors: Configure the bucket size of the phonebook.....	482
Menus: Modify the order of menus.....	482
Menus: Modify submenus.....	482
Object auto-naming settings.....	483
Configure the format of object names.....	483
SOXDocument object auto-naming settings for duplicate file names.....	485
Environment migration settings.....	485
Report fragment settings.....	485
Configuring your mail server.....	486
Date field display format.....	487
Configuring large files for upload.....	487
Enabling and configuring the opening of Microsoft Office files.....	488
Reviewing the Net Promoter Score (NPS) survey settings.....	490
Signature and lock settings.....	490
Object Reset settings.....	494
View settings.....	495
Bulk move and rename setting.....	497

Configure HTTP request logging for IBM Watson Language Translator.....	498
Custom settings.....	498
Creating a custom setting.....	499
Deleting a custom setting.....	499
Copying settings and folders	499
Common folder settings.....	500
Maximum rows in exchange rate upload file.....	500
Maximum page size.....	500
Exclude characters from user names.....	500
Set the system security model.....	500
Disable access control on Role groups.....	501
Configure self-contained object types.....	501
Platform folder settings.....	502
Enable custom REST service.....	502
Set the sign of an integer returned by dates function.....	503
Set the default pageSize for API queries.....	503
Set localization options.....	503
Configure primary associations.....	504
Configure the host setting.....	505
Cognos URL settings.....	505
Cross-context sharing.....	506
Platform Reporting Framework folder settings.....	507
Reporting Schema folder settings.....	507
Security settings.....	509
User Preferences folder settings.....	515
Set alert notification behavior.....	516

Chapter 21. Configuring the global search feature..... 517

Setting up global search.....	517
Setting login information for the search server.....	518
Changing the login information for the search server.....	520
Using OPBackup and OPRestore when global search is enabled.....	520
Enabling and disabling global search.....	521
Recreating the index for global search.....	522
Enabling and disabling file attachment searching.....	522
Enabling attachment file types for global search.....	522
Customizing global search.....	523
Enabling or disabling object types or fields for global search.....	523
Example: customizing global search on initial enablement.....	524
Example: adding or removing object types and fields with an already-enabled global search.....	525
Changing the database connection information for the search server.....	525
Displaying a custom field in global search results.....	526
Global search settings.....	527
Unhiding the hidden global search settings.....	527
Setting the Query Path to the global search administration server.....	528
Setting the URL to the global search administration server.....	528
Setting the progress refresh interval.....	528
Setting the number of records to cache.....	529
Setting the polling interval.....	529
Setting the number of records to cache before sending to the server for indexing.....	530
Setting the Query Path to the Apache Solr server that handles Folder ACL indexing.....	530
Setting the language analyzer that is used by search.....	530
Setting the Query Path to the Apache Solr server that handles Folder ACL indexing.....	531
Setting the URL to the Apache Solr server that handles Folder ACL indexing.....	531
Setting the number of records inserted per batch.....	532
Setting the Query Path to the Apache Solr server that handles Folder ACL search requests.....	532
Setting the URL to the Apache Solr server that handles OpenPages search requests.....	532

Setting the number of attempts to fill the search results.....	533
Setting the number of search results records that are cached per user session.....	533
Setting the internal page size for search results.....	533
Setting the URL to the Apache Solr server that handles search requests.....	534
Setting a time limit to search before timing out.....	534
Setting an additional field in the search result set.....	534
Setting whether to allow compression.....	535
Setting the network connection request timeout.....	535
Setting whether to allow URL redirects.....	535
Setting the number of allowed connections from the platform.....	536
Setting the number of allowed connections.....	536
Setting the number of times a request is reattempted.....	536
Setting the socket timeout for indexing.....	536
Setting the socket timeout for searching.....	537
Setting the Apache Solr password.....	537
Setting the Apache Solr user ID.....	537
Setting the default number of search results to return per page.....	537
The global search properties file.....	538
Setting the error handling parameters for the indexer.....	538
Setting the maximum opsearchtool.jar heap size.....	539
Setting the maximum Apache Solr heap size.....	539
Setting the maximum opsearchtool.jar heap size during indexing.....	539
Setting the maximum text extraction heap size for indexing.....	540
Setting the text extractor timeout limit.....	540
Setting the maximum text to extract from file attachments for indexing.....	541
Setting the root path location for file attachment search.....	541
Global search FAQs.....	542

Chapter 22. Using IBM OpenPages with Watson utilities with Db2 databases..... 545

Db2 and the OpenPages backup and restore utilities.....	545
Configuring backup job notification.....	545
Asynchronous background jobs and administrative functions.....	547
Enabling and disabling asynchronous background processes checking.....	548
The OPBackup utility (Db2).....	548
Backing up custom files.....	549
Enabling and disabling storage backup.....	549
Configuring OPBackup to use GZIP.....	550
Running the OPBackup command (Db2).....	550
The OPRestore utility (Db2).....	551
Running the OPRestore command.....	551
Using the Cognos Backup utility (Db2).....	552
The OpenPages with Watson file storage directory.....	552
Running the OPCCBackup command (Db2).....	553
Cognos backed-up content.....	553
Configuring OPCCBackup to use GZIP.....	553
Using the Cognos Restore utility.....	554
Running the OPCCRestore command.....	554
Database backup and restore for Db2.....	555
Restoring backed up production data in a new Db2 environment.....	556
Refreshing a test environment from backup files (Db2).....	558
Prerequisites to refreshing a Db2 test environment.....	558
Backup of production databases in OpenPages with Watson on the Db2 server	559
Backing up and copying OpenPages with Watson application production files for a Db2 database.....	559
Backup of OpenPages with Watson databases on the test server.....	559
Backing up OpenPages with Watson application files on your test server.....	559
Running the OPCCBackup command.....	559

Drop the Db2 database for the application on the test system.....	560
Copy and restore the production Db2 database backup file to the test Db2 database server.....	560
Update the OpenPages storage location in the Db2 database.....	561
Back up the Cognos database on the Db2 production and test servers.....	562
Back up Cognos configuration files on the Db2 production and test servers.....	562
Modify SSO and LDAP configuration in the test environment.....	563
Copy and restore the Cognos production database backup file to the test database server.....	563
Drop the Db2 database for Cognos on the Test Server.....	563
Copy custom deliverables to the test environment.....	564
Copy custom triggers	564
Copy other custom deliverables to the test environment.....	564
Starting OpenPages with Watson in the test environment.....	565
Updating the OPSysSystem password.....	565
Update database connection references for Cognos.....	565
Update URL host pointers for Cognos reports.....	565
Update the global search settings.....	565
Utilities for filtering on long string field content in a Db2 database.....	566
Enabling Db2 Text Search.....	567
Creating a long string index.....	568
Changing the index synchronizing job.....	570
Drop a long string index.....	571
Entity Move/Rename utility.....	572
Entity Move/Rename utility prerequisites.....	573
Configuring the Entity Move/Rename utility for a Db2 database.....	573
Prepare the input file for the Entity Move/Rename utility.....	574
Running the Entity Move/Rename utility interactively for a Db2 database.....	575
Running the Entity Move/Rename utility as a scheduled task.....	576
Impact of the Entity Move/Rename utility on the OpenPages application.....	576

Chapter 23. Using IBM OpenPages with Watson utilities with Oracle databases.. 577

Oracle databases and the backup and restore utilities.....	577
Prerequisite: Oracle client software.....	577
Oracle Data Pump.....	577
Configuring backup job notification.....	578
Asynchronous background jobs and administrative functions.....	579
Enabling and disabling asynchronous background processes checking.....	580
Encrypting database passwords in the backup-restore utility environment files.....	581
The OPBackup utility (Oracle).....	581
Modifying the backup-restore environment file.....	582
Backing up custom files.....	583
Running the OPBackup command (Oracle).....	583
Backing up the OpenPages database (Oracle).....	584
Running a live backup (Oracle).....	585
OpenPages with Watson backed-up content.....	586
Configuring OPBackup to use GZIP.....	586
Enabling and disabling storage backup.....	586
The OpenPages restore utility on the Oracle database.....	587
Running the OPRestore command.....	587
OPRestore log files.....	588
Using the Cognos backup utility.....	588
Oracle Data Pump configuration on a first time use.....	589
The OpenPages with Watson file storage directory.....	589
Configuring or updating the Oracle Data Pump directory.....	589
Running the OPCCBackup command.....	590
Cognos backed-up content.....	591
Configuring OPCCBackup to use GZIP.....	591
Using the Cognos restore utility.....	591

Running the OPCCRestore command.....	592
Using Oracle online database backup (RMAN) for point-in-time recovery.....	592
Oracle online database backups.....	593
Running Oracle online database backups (RMAN).....	593
Monitoring the size of the Oracle backup area.....	598
Adjusting the size of the Oracle backup area.....	598
Disabling online backup of the Oracle database instance.....	600
Performing Oracle online database crash recoveries.....	600
Refreshing a test environment from backup files.....	600
Backing up and copying the OpenPages with Watson application production files for an Oracle database.....	601
Backing up the OpenPages with Watson application test files on your Oracle test data.....	601
Deleting data on the test database system.....	601
Copy the production database dump (.dmp) file to the test database server.....	601
Import the production data into the test environment.....	602
Update the OpenPages with Watson storage location in the Oracle database.....	603
Update the global search settings.....	605
Update Cognos data in the test environment.....	606
Modify SSO and LDAP Configuration in the test environment.....	609
Copy custom triggers	609
Copy other custom deliverables to the test environment.....	610
Starting OpenPages with Watson in the test environment.....	610
Updating the OPSSystem password.....	610
Update URL host pointers for Cognos reports.....	610
Utilities for filtering on long string field content in an Oracle database.....	610
Create a long string index for an Oracle database.....	611
Enabling Oracle Text.....	612
Create a schedule job to synchronize a long string index.....	613
Drop a long string index.....	614
Modifying the list of stop words.....	615
String concatenation utility.....	616
Running string concatenation.....	616
The string concatenation SQL file.....	617
Entity Move/Rename utility.....	622
Entity Move/Rename utility prerequisites.....	622
Configuring the Entity Move/Rename utility for an Oracle database.....	622
Prepare the input file for the Entity Move/Rename utility.....	623
Running the entity move/rename utility interactively.....	625
Running the Entity Move/Rename utility as a scheduled task.....	626
Impact of the Entity Move/Rename utility on the OpenPages application.....	626
Chapter 24. System Maintenance.....	627
Application server restrictions.....	627
Port assignments.....	627
Change default port numbers.....	629
Checking port number availability.....	630
Changing application port numbers.....	630
Updating port values in the database.....	632
Updating port values on the reporting server.....	632
Updating URL host pointers for reports.....	633
Auditing configuration changes.....	634
Accessing the Configuration Audit report.....	634
The Configuration Audit report.....	634
Changing the password of the WebSphere Liberty keystore.....	635
Changing the keystore that is used by WebSphere Liberty.....	636
Changing the keystore that is used by Db2.....	636
Changing the OPSSystem password.....	637

Changing database password references.....	637
Change database password references on the OpenPages with Watson application server.....	638
Modifying the OpenPages database password in Cognos	639
Modifying database passwords in the backup-restore environment files.....	640
Updating the Oracle Enterprise Manager tool.....	641
Changing database name references.....	641
Testing the connection to the OpenPages database from the Oracle database client.....	642
Modifying the data source connection URL.....	642
Modify database references in the application configuration files.....	643
Modify database connection references for the reporting server.....	644
Storing passwords in a vault.....	646
TLS for OpenPages with Watson environments.....	649
Accessing the OpenPages with Watson application using TLS.....	650
Verifying TLS ports on application servers.....	650
Generating a Certificate Signing Request file.....	650
Importing signed CA certificates.....	650
Importing the CA certificate for the Java Runtime Environment of IBM Cognos Analytics.....	652
Installing CA certificates for all client browsers.....	652
Updating properties files so web browsers use the HTTPS protocol and TLS ports.....	653
Enabling secure session cookies on WebSphere Liberty.....	654
TLS configuration for Microsoft Internet Information Services.....	654
TLS configuration for Apache Web Server.....	656
TLS configuration on a Linux load balancer server	658
TLS configuration for CommandCenter for an Apache load balancer server (Windows).....	661
TLS configuration for Cognos for IBM HTTP Server	663
Configuring Cognos to connect to OpenPages by using TLS.....	665
TLS configuration for Db2.....	666
Modifying the LDAP configuration file for LDAP over TLS.....	669
Renewing TLS certificates for OpenPages with Watson.....	671
Setting up a secure connection for the global search service.....	673
Enabling a secure connection between the search server and the database server.....	676
Disabling the TLS database connection between the search server and the database server.....	677
Db2 native encryption.....	677
Oracle Transparent Data Encryption (TDE).....	677
Prerequisites and process overview.....	678
Encrypting OpenPages and Cognos table spaces.....	679
Shortening the OpenPages application URL.....	683
Parameters for cluster members.....	684
Configuring HTTP compression in OpenPages with Watson	685
Enabling or disabling HTTP compression on application servers.....	685
Enabling or disabling compression on the reporting server (Windows IIS).....	685
Enabling compression on the reporting server (Apache Web Server).....	686
Disabling compression on the reporing server (Apache Web Server).....	687
Factors that affect performance of views.....	688
Server tuning settings.....	688
Changing JVM options on application servers.....	688
Configuring the reporting server.....	689
Configuring the database (Db2).....	689
Improve the performance of OpenPages application functions on a Db2 server.....	691
Installing tools and utilities (IBM OpenPages with Watson).....	692
Using log files.....	693
Configuring extended access logging on WebSphere Liberty.....	693
Gathering logs with the LogCollector user interface.....	693
Gathering logs with the log collector tool.....	694
OpenPages with Watson standard log files.....	696
Viewing information about background processes.....	703
Troubleshooting browser issues.....	704
Optimizing application performance in Microsoft Edge browsers.....	704

Setting a session inactivity timeout value.....	704
Setting the Cognos application firewall for browser security.....	706
Browser security issues and running reports.....	707
Browser locale settings and messaging issues.....	707
Browser errors about Content Security Policy.....	707
Browser best practices.....	707
Chapter 25. Starting and stopping servers.....	709
Starting application servers.....	709
Starting application servers by using Windows services.....	709
Starting all application services by running a script (Windows).....	710
Starting all application servers by running a script (Linux).....	710
Determining application readiness.....	711
Stopping application servers.....	711
Stopping application servers by using Windows services.....	711
Stopping all application servers in Windows by using a script.....	711
Stopping all application servers on Linux by using a script.....	712
Start or stop the global search services.....	712
Starting the global search services by using a script.....	712
Stopping the global search services by using a script.....	713
Starting the global search services on Windows.....	713
Starting the global search services on Linux.....	714
Stopping the global search services.....	715
Start or stop the database services.....	715
Starting and stopping the Oracle database server in a Windows environment.....	715
Starting and stopping the Oracle database server in Linux environments.....	716
Starting and stopping the Cognos services.....	717
Using the IBM Cognos configuration tool to start and stop the IBM Cognos service.....	717
Using the Windows operating system to start and stop the IBM Cognos service.....	717
Using the Linux operating system to start and stop the IBM Cognos service.....	718
Chapter 26. Migrating OpenPages environments.....	719
Settings that apply to environment migration.....	719
Supported migration items.....	720
Exporting dependencies.....	722
Items that are not migrated.....	722
Item dependencies not migrated by default.....	725
Environment migration best practices.....	725
The environment migration process.....	726
Exporting configuration items from the source environment.....	727
Importing configuration items to the target environment.....	727
Configuring environment migration to allow special characters.....	728
Validating a migration file.....	728
Importing a migration file	729
Chapter 27. Using ObjectManager.....	731
Working with loader files.....	731
Creating a data loader file.....	732
Running ObjectManager commands.....	732
ObjectManager command line parameters.....	733
Load command example.....	734
Dump command example.....	735
Batch loader file syntax and sample.....	735
Using ObjectManager to move objects.....	736
Using ObjectManager to rename objects.....	737
Using ObjectManager to assign or revoke role assignments.....	739
Using ObjectManager to create or load users.....	741

Modifying ObjectManager properties.....	742
Settings in the ObjectManager.properties file	743
Filtering data for export.....	748
Before you begin.....	749
About the filters configuration file.....	749
Predefined filters.....	749
Controlling data load behavior.....	751
Managing currency exchange rates.....	752
Importing exchange rates.....	752
Exporting all currency exchange rates.....	753
Enabling and disabling currencies.....	753
Importing currency field definitions.....	754
Exporting currency field definitions.....	755
Importing computed field definitions.....	755
Exporting computed field definitions.....	756
Exporting file attachments.....	756
Importing file attachments.....	757
Migrating configuration changes using the ObjectManager tool.....	760
The ObjectManager migration process.....	760
Modifying ObjectManager settings.....	761
Migrating configuration changes.....	763

Chapter 28. FastMap.....	767
FastMap overview.....	767
The FastMap import process.....	768
FastMap templates.....	768
The FastMap data validation process.....	769
FastMap localization.....	769
Accessing FastMap to import data and view status.....	770
Resolving FastMap validation errors.....	771
Understanding FastMap validation errors.....	771
Troubleshooting FastMap conflict with recent updates warning message.....	771
Troubleshooting FastMap validation messages.....	772
Creating FastMap import templates.....	776
The data exported to a workbook by FastMap.....	777
Working with data load worksheets.....	777
Defining paths for objects.....	777
Using special column headings.....	778
Defining property fields for objects in FastMap templates.....	779
Guidelines for entering object data into FastMap templates.....	779
Adding custom columns and worksheets to FastMap templates.....	781
Sample Object worksheet for updating and creating objects.....	781
Sample self-contained object worksheet.....	782
Sample Business Entity worksheet for creating a new business entity structure.....	783
Using the FastMap Definition worksheet.....	783
Unhiding a FastMap Definition worksheet.....	784
FastMap parameters.....	784
FastMap export templates.....	784
Modifying parameters in the default FastMap export template.....	784
Specifying a FastMap export template.....	785
FastMap parameters for importing and exporting data.....	786
Configuring a lookup key for FastMap	793
Modifying export settings to optimize FastMap performance.....	795
Limiting the rows for import to optimize FastMap performance.....	795
Setting a transaction timeout to optimize FastMap performance.....	795
Adding a processing delay to optimize FastMap performance.....	796
Securing FastMap import templates stored on the server.....	796

Cleaning up FastMap import templates stored on the server.....	797
Using FastMap with questionnaire template and assessment objects.....	797
Exporting and importing tags with FastMap.....	798
Chapter 29. Configuring and generating the reporting framework.....	799
The reporting framework	799
Framework models.....	799
Namespaces	800
Triangle object relationships.....	801
Recursive object levels.....	802
Planning the configuration.....	806
Configuring settings that apply to all framework models.....	806
Configuring the number of models that can be concurrently generated.....	806
Including workflow fields	807
Adding locale codes to the reporting framework	807
Defining the sort order locale	807
Setting the triangle reporting framework object relationships.....	808
Enabling the reporting framework for object types.....	809
Defining the transaction timeout for reporting framework generation.....	809
Defining how security checks are applied during reporting framework generation.....	809
Configuring framework models	810
Creating a framework model and namespace using a template	810
Defining a name for a framework model.....	810
Defining the format for a framework model.....	811
Enabling a framework model	811
Defining the query mode for a framework model	811
Defining the package label for a framework model	812
Defining whether a framework model uses profile filtering.....	812
Configure reporting framework namespaces.....	812
Defining a name for a reporting framework namespace.....	812
Defining the object model for a namespace	813
Setting a namespace as the default	814
Enabling a namespace.....	814
Defining entity recursive object levels for a namespace.....	814
Generating the reporting framework	814
Reporting framework permissions.....	816
Choosing update options in the reporting framework.....	816
Updating the reporting framework.....	817
Viewing reporting framework details.....	817
Chapter 30. SDI connectors.....	819
IBM QRadar integration.....	819
Using the QRadar integration project.....	820
Configuring email notifications to be sent from the QRadar assembly line connector components.....	820
Specifying a primary parent ID to the OpenPages connector.....	821
Specifying currency values to the OpenPages connector by the output mapping.....	824
Specifying date values to the OpenPages connector via the output mapping.....	824
IBM OpenPages SDI Connector for UCF Common Controls Hub integration.....	824
Run the UCF assembly lines.....	825
IBM Security Directory Integrator (SDI) techniques.....	826
Scheduling Security Directory Integrator.....	826
Security Directory Integrator command line tips.....	826
Troubleshooting the assembly line "Connection refused" error.....	827
Chapter 31. Configuring questionnaire assessments.....	829

Chapter 32. Configuring OpenPages Loss Event Entry.....	831
Planning the configuration	831
Designing the loss entry form.....	833
How users are handled.....	833
Where loss events get created.....	833
Who loss events get assigned to	834
How dates are validated.....	835
How to launch OpenPages Loss Event Entry	835
How confirmation emails are configured.....	837
Configuring the Loss Event Entry app.....	839
Chapter 33. Configuring IBM Watson Integrations.....	843
IBM Watson Assistant	843
Configuring a web chat assistant by using IBM Watson Assistant.....	843
Configuring the integration between an assistant and OpenPages	844
Enabling additional security features for IBM Watson Assistant on IBM Cloud.....	845
IBM Watson Language Translator.....	847
Configuring IBM Watson Language Translator on IBM Cloud.....	849
Configuring the integration between IBM Watson Language Translator and OpenPages	849
Natural language processing services	850
Configuration overview for natural language classifier services.....	852
Configuring Watson Discovery	853
Configuring a Natural Language Understanding service on IBM Cloud.....	853
Defining a classifier configuration.....	854
Defining a classifier field.....	855
Monitoring and downloading classifier data usage	856
Configuring a proxy URL for authentication (IBM Cloud).....	857
Custom Machine Learning Models.....	857
What you need to configure your model.....	858
Setting up a connection to your model.....	859
Configuring model inputs.....	862
Configuring model outputs.....	863
Configuring user guidance.....	871
Adding a model to a view.....	872
Testing a model.....	873
Importing a certificate for Cloud Pak for Data services.....	874
Chapter 34. IBM OpenPages Data Privacy Management.....	877
Configuring the Watson Knowledge Catalog connector.....	878
Chapter 35. IT Governance with RiskLens.....	881
Configuring RiskLens.....	882
Chapter 36. IBM OpenPages Model Risk Governance.....	885
Loading the AI Factsheets files.....	885
Configuring the integration.....	886
Setting up OpenPages to connect to RabbitMQ.....	889
Sample trigger configuration.....	889
Chapter 37. Configuring IBM OpenPages Regulatory Compliance Management....	893
Ascent Connector.....	893
Configuring the Ascent connector.....	893
Reloading Ascent data.....	894
Thomson Reuters Connector.....	895
Preparing the SFTP server.....	896

Configuring the feeds.....	896
Configuring the Thomson Reuters import.....	897
Thomson Reuters taxonomy mapping.....	899
Reg-Track connector.....	901
Configuring the Reg-Track connector.....	902
Reg-Track taxonomy mapping.....	903
Wolters Kluwer Connector.....	906
Configuring the Wolters Kluwer import.....	907
Wolters Kluwer taxonomy mapping.....	908
Processing regulatory events by using rules.....	911
Creating rules.....	911
Copying a rule.....	914
Enabling and disabling rules.....	914
Editing rules.....	915
RCM Theme Deployer.....	915
Process overview for the RCM Theme Deployer.....	916
Setting up auto-naming for RCM objects.....	916
Updating views for the RCM Theme Deployer.....	916
Using the RCM configuration tool.....	917
Chapter 38. Configuring IBM OpenPages Third Party Risk Management.....	919
SecurityScorecard connector.....	919
Configuring the SecurityScorecard connector.....	919
Supply Wisdom connector.....	920
Configuring the Supply Wisdom connector.....	921
RapidRatings connector.....	921
RiskRecon connector.....	922
Configuring RiskRecon.....	922
Appendix A. The Notification Manager.....	925
Requirements for setting up a notification.....	925
Setting up a notification.....	926
Task 1: Creating a page template	926
Task 2: Creating the notification.....	926
Task 3: Triggering the notification.....	927
Appendix B. Properties and parameters.....	931
Aurora properties and parameters.....	931
OpenPages server properties and parameters.....	933
Sosa properties and parameters	934
Tools properties and parameters	934
Appendix C. Troubleshooting and support	937
Techniques for troubleshooting problems.....	937
Searching knowledge bases.....	938
Getting fixes.....	939
Contacting IBM Support.....	939
Exchanging information with IBM.....	940
Sending information to IBM Support.....	941
Receiving information from IBM Support.....	941
Subscribing to Support notifications.....	941
Missing Administration menu items.....	942
Known problems and solutions for global search.....	942
Global search start fails.....	942
Global search setup fails.....	943
Forcing a reset of global search.....	943
Checking for global search setup issues and periodic monitoring.....	945

Before you contact IBM OpenPages Support.....	945
QRadar integration package.....	946
SDI properties file error message.....	946
Do not include security domain groups when creating object filters or security rule formulas.....	946
Objects can be saved with an empty required field.....	946
JSON file might not display multibyte characters correctly in Wordpad.....	947
Remediating after an Enumerated String field is changed to a multi-select field (Db2).....	947
System delay when modifying object types and fields (Db2).....	947
NoClassDefFoundError errors when you run custom code.....	948
Risk Assessment Summary report does not show related risks and controls.....	949
Changing the settings for ORM.....	949
Troubleshooting helpers.....	950
Users or group properties are overwritten in IBM OpenPages for IBM Cloud Pak for Data.....	950
Appendix D. Best practices for configuring IBM OpenPages with Watson	953
Use short field names and field group names.....	953
Limit the number of security rules and complexity of security rules.....	953
Limit the number of SOXBusEntity objects in the system.....	953
Be aware of shared field groups.....	953
Eliminating unused object type relationships.....	954
Task-oriented hyperlinking.....	954
Appendix E. Creating custom actions for GRC workflows.....	957
Appendix F. Personal information processed and stored by OpenPages.....	961
Appendix G. Legacy features	963
Legacy registry settings.....	963
Legacy application permissions.....	964
Legacy FastMap import parameters.....	965
Notices.....	967
Glossary.....	971
Index.....	973

Introduction

The *IBM OpenPages with Watson Administrator's Guide* is intended for use with IBM OpenPages® with Watson™ on-premises and on cloud. The content contains instructions for maintaining, configuring, and administering the OpenPages application. It is intended for use by administrators who have a background in systems management. Topics include user and group administration, database backup and restoration, customizing the application's look and feel, and using the data loader capabilities.

IBM OpenPages with Watson documentation

IBM® maintains one set of documentation serving IBM OpenPages with Watson, IBM OpenPages for IBM Cloud Pak for Data, and IBM OpenPages with Watson on Cloud deployments. The IBM OpenPages with Watson documentation describes certain features and functions which may not be available on the cloud.

If you have any questions about the functionality available in the product version that you are using, contact IBM OpenPages Support by using the [IBM Support portal](#).

Accessibility features

Accessibility features help users who have a physical disability, such as restricted mobility or limited vision, to use information technology products. OpenPages documentation has accessibility features. PDF documents are supplemental and include no added accessibility features.

Database tool information

IBM OpenPages with Watson supports both the IBM Db2® database and the Oracle database. (Oracle is not supported in IBM OpenPages for IBM Cloud Pak for Data).

- To run OpenPages with Watson SQL scripts, you must use CLPPlus with Db2, and SQL*Plus with Oracle database.
- To run queries, you can use any SQL tool that is compatible with the database. For example, you could use CLPPlus or Optim™ Development Studio to run queries on the Db2 database.

Chapter 1. IBM OpenPages with Watson

IBM OpenPages with Watson is an AI-driven, highly scalable governance, risk, and compliance (GRC) solution. OpenPages enables organizations to centralize siloed risk management functions within a single environment to identify, manage, monitor, and report on risk and regulatory compliance.

OpenPages serves as the foundation for a company's enterprise risk management (ERM) efforts by unifying enterprise-wide risk and compliance initiatives into a single management system. With its solutions for areas such as ESG, data privacy, operational risk and more, OpenPages with Watson provides a modular and integrated approach to governance, risk, and compliance.

Each component provides a highly configurable capability that supports your specific methodology, without having to write custom code, whether in loss events, KRI, or any other solution component. The result is that companies can embed risk management into the business and improve outcomes over time.

IBM OpenPages with Watson solutions

IBM OpenPages with Watson consists of the following solutions:

- IBM OpenPages Operational Risk Management (ORM) provides a fully integrated operational risk solution, including risk control self-assessments (RCSAs), key risk indicators, (KRIs), loss event data management, and advanced reporting and business intelligence with IBM Cognos® finance integrated risk management. Dashboard components are available to provide an enterprise-wide view of risk across the business and manage Basel II AMA compliance in the banking industry.
- IBM OpenPages Business Continuity Management (BCM) is used by an organization, or group, to maintain or resume a predetermined level of operations during or after a disruptive event. All risks that can potentially impact the business during or following an event are identified.
- IBM OpenPages Data Privacy Management (DPM) is used by an organization to aid in complying with data privacy regulations. Using DPM, organizations can have clear visibility of all their private or sensitive data and ensure that the data is being handled correctly.
- IBM OpenPages Risk Management for ESG (ESG) is used by an organization to help manage their environment, social and governance priorities, strategic objectives, and compliance.
- IBM OpenPages Financial Controls Management (FCM) reduces the time and resource costs that are associated with ongoing compliance for financial reporting regulations.
- IBM OpenPages Model Risk Governance (MRG) supports organizations in organizing and centralizing their Model Inventory.
- IBM OpenPages Policy Management (PCM) provides an integrated solution for reducing the complexity of complying with numerous industrial, ethics, privacy, and government regulatory mandates.
- IBM OpenPages IT Governance (ITG) provides a risk-based, policy-driven approach to managing risk and compliance initiative for the IT organization.
- IBM OpenPages Internal Audit Management (IAM) provides an integrated audit management solution to manage the full life cycle of internal audits.
- IBM OpenPages Regulatory Compliance Management (RCM) supports organizations in breaking down regulations into a catalog of requirements, evaluating its impact to the business, and creating actionable tasks.
- IBM OpenPages Third Party Risk Management (TPRM) supports firms in assessing and analyzing risks that are associated with the vendors they do business with.

How IBM OpenPages with Watson can help

The OpenPages with Watson application provides many capabilities to simplify and centralize compliance and risk management activities.

Shared content management and common repository

- Logically presents processes, risks and controls in many-to-many and shared relationships at multiple levels that can be configured to your business processes
- Supports importing existing corporate data and maintains a complete audit trail and version history
- Ensures consistent regulatory enforcement and monitoring across multiple regulations.

Dynamic decision support with Cognos

- Delivers rich, interactive, real-time executive dashboards and reports
- CrossTrack enables drill-down from reports into supporting reports as well as the underlying detail data
- Provide organizational assurance for regulatory compliance

Simple configuration and localization

- Detail user-specific tasks and actions on a personal home page.
- Reduce training costs with intuitive navigation, easy-to-use web-based layout, and localized text in English (both UK and US), French, Italian, Spanish, German, Japanese, Simplified Chinese, Traditional Chinese, and Brazilian Portuguese.
- Lower administration costs with simple browser based configuration capabilities managed by administrators for end-users.

Flexible automation

- Streamlined compliance procedures and automated sub-certifications without sacrificing risk.

Web services-based integration

- OpenAccess API Interoperates with leading third-party applications to enhance policies and procedures with actual business data
- Reduced total cost of ownership and easy integration with existing corporate compliance management systems

Show me

This video provides an overview of OpenPages.

[OpenPages Overview](#)

This video provides an overview of AI in OpenPages.

[OpenPages and AI](#)

Installation locations (on prem)

The installation directory is the location of product artifacts after a package, product, or component is installed. The following table lists the conventions that are used to refer to the installation location of installed components and products:

Important: Directory locations that contain spaces are not supported. IBM OpenPages with Watson or any software that is used by it must not be installed into a directory with spaces. For example, do not install database server, database client, or application server software into the Program Files directory.

If you're using IBM OpenPages for IBM Cloud Pak for Data, see [Files and directories in IBM OpenPages for IBM Cloud Pak for Data](#).

Table 1. Variable notations for installation directories

Directory	Description
<installation_server_home>	<p>The directory where the IBM OpenPages with Watson installation server is installed.</p> <p>For example:</p> <ul style="list-style-type: none"> On Windows: C:\IBM\OPInstall\OP_<version>_Installer On Linux®: /home/opuser/IBM/OPInstall/OP_<version>_Installer
<agent_home>	<p>The directory where the IBM OpenPages with Watson installation agent is installed on a remote server.</p> <p>For example:</p> <ul style="list-style-type: none"> On Windows: C:\IBM\OPAgent On Linux: /home/opuser/IBM/OPAgent
<OP_HOME>	<p>The directory where OpenPages with Watson is installed.</p> <p>For example:</p> <ul style="list-style-type: none"> On Windows: C:\IBM\OpenPages On Linux: /opt/opuser/IBM/OpenPages <p>In the installation app, you specify the <OP_HOME> directory in the OP Home Directory field each Application Server card.</p>
<ORACLE_HOME>	<p>The installation location of the Oracle database software.</p> <p>For example:</p> <ul style="list-style-type: none"> On Windows: <ul style="list-style-type: none"> C:\app\oracle\product\19.3.0\client_1 (Oracle Admin Client) C:\oracle\instantclient_19_9 (Oracle Instant Client) C:\app\oracle\product\19.3.0\dbhome_1 (server) On Linux: <ul style="list-style-type: none"> /home/oracle/app/oracle/product/19.3.0/client_1 (Oracle Admin Client) /home/oracle/instantclient_19_9 (Oracle Instant Client) /home/oracle/app/oracle/product/19.3.0/dbhome_1 (server)
<DB2_HOME>	<p>The installation location of the IBM Db2 software.</p> <p>For example:</p> <ul style="list-style-type: none"> On Windows: C:\IBM\SQLLIB On Linux: /home/db2inst1/sqllib

Table 1. Variable notations for installation directories (continued)

Directory	Description
<WLP_HOME>	<p>The installation location of IBM WebSphere® Liberty.</p> <p>For example:</p> <ul style="list-style-type: none"> • On Windows: <OP_HOME>\wlp • On Linux: <OP_HOME>/wlp
<WLP_USER_HOME>	<p>The location of OpenPages with Watson application files and server configuration files.</p> <p>For example:</p> <ul style="list-style-type: none"> • On Windows: <OP_HOME>\wlp-user • On Linux: <OP_HOME>/wlp-user
<COGNOS_HOME>	<p>The installation location of IBM Cognos Analytics.</p> <p>For example:</p> <ul style="list-style-type: none"> • On Windows: C:\IBM\cognos\analytics • On Linux: /usr/IBM/cognos/analytics
<JAVA_HOME>	<p>The installation location of IBM SDK, Java™ Technology Edition or Java Runtime Environment (JRE).</p> <p>IBM SDK example on an application server:</p> <ul style="list-style-type: none"> • On Windows: C:\IBM\java_8.0_64 • On Linux: /opt/IBM/java_8.0_64 <p>JRE example on a reporting server where IBM Cognos Analytics is installed:</p> <ul style="list-style-type: none"> • On Windows: C:\IBM\cognos\analytics\ibm-jre\jre • On Linux: /usr/IBM/cognos/analytics/ibm-jre/jre <p>IBM SDK example on a search server:</p> <ul style="list-style-type: none"> • On Windows: C:\IBM\java_8.0_64\ • On Linux: /opt/IBM/java_8.0_64/
<CC_HOME>	<p>The installation location of OpenPages with Watson CommandCenter.</p> <p>For example:</p> <ul style="list-style-type: none"> • On Windows: C:\IBM\OpenPages\CommandCenter • On Linux: /opt/IBM/OpenPages/CommandCenter

Table 1. Variable notations for installation directories (continued)

Directory	Description
<SEARCH_HOME>	<p>The installation location of global search.</p> <p>The <SEARCH_HOME> directory contains the opsearchtools.jar, Apache Solr, and other global search files. The global search indexing directory is also stored in the <SEARCH_HOME> directory.</p> <p>For example:</p> <ul style="list-style-type: none"> On Windows: C:\IBM\OpenPages\OPSearch On Linux: /opt/IBM/OpenPages/OPSearch <p>In the installation app, you specify the <SEARCH_HOME> directory in the Search Home Directory field on the Search Server card.</p>

Special characters in passwords

You can use certain special characters in certain passwords.

The special characters that you can use in passwords are:

```
. + - [ ] * ~ _ # : ?
```

Note: Spaces are not supported.

You can use these special characters in database user passwords and operating system accounts for database schema owners.

If you use special characters in passwords, you must surround the password in quotation marks. Use the following syntax:

IBM Db2 connection strings

For Db2 databases, when you provide a password in a connection string, use the following syntax:

On Linux, use \' around the password. For example:

```
clppplus -nw openpage\'DB~Password\'@host:50000/opx
```

On Windows, use single quotation marks around the password:

```
clppplus -nw openpage'DB~Password'@host:50000/opx
```

IBM Db2 script parameters in CLPPlus

For Db2 databases, when you provide a password in a script parameter, use the following syntax:

On Linux, use one of the following options:

- Use \' around the password. For example:

```
clppplus -nw @sql-wrapper CustomIndexing_Step1_AddTextIndexing_to_DB.sql
/tmp/log.log c6de0652985e:50000/OPX db2inst1 \'DB~Password\' openpage
```

- Use \" around the password:

```
clppplus -nw @sql-wrapper CustomIndexing_Step1_AddTextIndexing_to_DB.sql
/tmp/log.log c6de0652985e:50000/OPX db2inst1 \"DB~Password\" openpage
```

On Windows, use one of the following options:

- Use ' around the password. For example:

```
clppplus -nw @sql-wrapper CustomIndexing_Step1_AddTextIndexing_to_DB.sql
```

```
/tmp/log.log server.corp.com:50000/OPX db2admin 'DB~Password' openpage
```

- Use \" around the password:

```
clppplus -nw @sql-wrapper CustomIndexing_Step1_AddTextIndexing_to_DB.sql  
/tmp/log.log server.corp.com:50000/OPX db2admin \"DB~Password\" openpage
```

Db2 utilities

When you run Db2 utilities, such as db2 connect or db2rbind, do not use quotation marks around passwords.

Oracle connection strings

For Oracle databases, when you provide a password in a connection string, use \" around the password. For example:

```
sqlplus sys\"DB~Password\"@op as dba
```

Oracle script parameters in SQL*Plus

For Oracle databases, when you provide a password in a script parameter, use the following syntax:

- On Windows, use double quotation marks around the password.

```
sqlplus /nolog @sql-wrapper.sql  
update-storage c:\temp\upd-storage-output.log  
op openpages "pass~word" LFS eng11 eng11  
Windows c:\OpenPages\openpages-storage
```

- On Linux, use single quotation marks around the password.

```
sqlplus /nolog @sql-wrapper.sql  
update-storage /home/op/upd-storage-output.log  
op openpages 'pass~word' LFS eng11 end11  
Unix /usr/opdata/openpages-storage
```

Installation scripts, tools, and utilities

For tools and utilities that take the password as a parameter, use the following syntax:

- On Windows, use double quotation marks around the password.

```
op-validate-dba-install.bat "DB~Password"
```

- On Linux, use single quotation marks around the password.

```
./op-validate-dba-install.sh 'DB~Password'
```

Passwords in property files

For .env files and .properties files, do not use any quotation marks around passwords.

Variables and placeholders

When you run commands in IBM OpenPages with Watson, you need to know the values for various variables or placeholders.

For example, a command might require you to enter the <server_name> of an application server. The following table shows you how to find this value by looking in the deploy.properties file or in the installation app.

Table 2. Variables in commands (IBM OpenPages with Watson)

Parameter	Where to find it
<OP_HOME>	<ul style="list-style-type: none">In the deploy.properties file: in each [app.server<N>] section, op_home_directoryIn the installation app: on each Application Server card, OP Home Directory

Table 2. Variables in commands (IBM OpenPages with Watson) (continued)

Parameter	Where to find it
<server_name>	<ul style="list-style-type: none"> In the deploy.properties file: in each [app.server<N>] section, op_server_name In the installation app: Application ServerN card: OP Server Name <p>When you reference an application server, you use the format <server_name>Server<N>. For example, suppose OP Server Name on the Application Server1 card is set to opapp. The full name of the admin application server is:opappServer1.</p>

Chapter 2. What's new?

New and changed features affect the administration of IBM OpenPages with Watson.

For information about all new features for this release, see the *IBM OpenPages with Watson New Features Guide*.

For an up-to-date list of environments that OpenPages with Watson supports, see the [Supported Environments](#) web page.

New and changed features in version 9.0.0.0

New and changed features in version 9.0.0.0 are described in the following tables.

For more information, see the *IBM OpenPages with Watson New Features Guide*.

Platform enhancements

Table 3. Platform enhancements	
For information about...	See topic...
You can now export the following items by using Export Configuration : <ul style="list-style-type: none">• Groups and users• Role templates• Role assignments You can also import these items.	“Supported migration items” on page 720
You can now give profiles localized names and descriptions.	“Creating a profile ” on page 220 “Editing a profile” on page 222
FastMap import files must now be in .xlsx format. The .xls format is no longer supported.	Chapter 28, “Using FastMap,” on page 767
FastMap export templates must now be in .xlsx format. The .xls format is no longer supported.	“FastMap export templates” on page 784
When you define a condition for a workflow or calculation, you can now choose starts with or ends with as an operator.	
When you configure validations for workflow actions, you can specify a custom error message that is displayed when the validation condition is not met.	“Defining a workflow action” on page 407
The implementation of WalkMe that is integrated with OpenPages is now enabled by default.	If you want to disable WalkMe, see “Integrating WalkMe” on page 238 .
The behavior of filter rules, which are used in grid relationship actions in views, has changed. A filter rule that compares folders now returns objects only if they are in the folder that you specify. Objects in subfolders are no longer included in the filter rule results.	“Defining dynamic filters on actions in relationship fields” on page 317

Administration and serviceability enhancements

Table 4. Administration and serviceability enhancements

For information about...	See topic...
<p>The names of the color settings for themes are now easier to understand.</p>	<p>“Defining custom themes” on page 243</p>
<p>Updating the Cognos URL by using settings.</p> <p>When you need to change the Cognos URL, you now update settings in OpenPages. You no longer need to update the <code>aurora.properties</code> file on each server.</p> <p>The following properties in <code>aurora.properties</code> have been replaced by settings:</p> <ul style="list-style-type: none"> • <code>cognos.server</code> is replaced by <code>/Platform/Reporting/Cognos Dispatcher Service URL</code> • <code>cognos.computation.server</code> is replaced by <code>/Platform/Reporting/Cognos SDK URL</code> • <code>logout.url.cognos</code> is replaced by <code>/Platform/Reporting/Cognos Logout URL</code> registry setting 	<p>“Configure the Cognos URL settings” on page 505</p> <p>“Aurora properties and parameters” on page 931</p>
<p>The new parameter for URL configuration strings: <code>dontPromptForUnsavedChanges</code></p> <p>By default, when users click a link to launch a helper, they receive a prompt to save their work if they've edited a task view and have not saved their changes. You can now disable this prompt.</p>	<p>“Attributes in the URL configuration string” on page 189</p>
<p>When you export fields by using ObjectManager or Environment Migration, the display type is included in the export.</p> <p>For example, when you export a user/group field, the XML file includes <code>displayType</code>, such as:</p> <pre data-bbox="246 1389 649 1438"><displayType name="Multi Valued User Selector" ...></pre> <p>If a field exists in a target system, you can update its <code>displayType</code> by importing the field. You no longer need to import the profiles that use the field. In the XML file, you can specify the <code>displayType</code> of the field or leave <code>displayType</code> out. If you don't specify a <code>displayType</code> in the field definition, the <code>displayType</code> from the profile is used.</p> <p>If a field does not exist in a target system, in addition to importing the field, you must import at least one object type and one profile that use the field. Otherwise, you will need to update the display type manually in the UI.</p>	

Table 4. Administration and serviceability enhancements (continued)

For information about...	See topic...
The ObjectManager property configuration. manager.dump.actor.object.profile. associations now exports groups and their assigned profiles.	“Settings in the ObjectManager.properties file” on page 743
The new setting Platform/API/Query/Default PageSize lets you control the default pageSize for queries through the API (REST API and Java API). The default value is 50.	“Set the default pageSize for API queries” on page 503 For more information, see the <i>IBM OpenPages with Watson Developer Guide</i> .
The new setting Platform > Reporting Framework V6 > Configuration > Datasource QS Security Filter defines how security checks are applied to query subjects during framework generation.	“Defining how security checks are applied during reporting framework generation” on page 809
The following properties are not used and have been removed from the aurora.properties file: <ul style="list-style-type: none">• database.pool.minsize• database.pool.maxsize• database.pool.refresh.interval	“Aurora properties and parameters” on page 931
The permissions on the Reporting folder under  > System Configuration > Pages and Templates have changed. By default, only members of the OPAdministrators group have Read, Write, Delete, and Mange permissions on the Reporting folder. Members of the OpenPagesApplicationUsers group have Read access.	
The new Show rule analysis feature displays information about the security rules for object types. The information can help you to understand the performance impact of security rules.	“Best practices for security rules” on page 102
For each object type, you can have one READ record level security rule that is enabled.	“Defining record level security rules” on page 85
In fresh installations, NPS is now enabled by default. Also, if you upgrade to 9.0 from a version prior to NPS being available, NPS is enabled by default. If you migrate, your previous NPS settings are retained.	“Configuring a Net Promoter Score survey” on page 239
When you load file attachments by using ObjectManager, you no longer need to specify the fileType in the loader file. OpenPages now uses the shortName to determine the fileType.	“Importing file attachments” on page 757

Documentation enhancements

A new Developer Guide had been added to the documentation set for IBM OpenPages with Watson 9.0.0.0. The Developer Guide contains the documentation and samples that developers need to interact programmatically with IBM OpenPages with Watson. The *OpenPages API documentation* section in the Administration Guide has been moved to the Developer Guide.

New and changed features in version 8.3.0.2

New and changed features in version 8.3.0.2 are described in the following tables.

For more information, see the *IBM OpenPages with Watson New Features Guide*.

Platform enhancements

Table 5. Platform enhancements	
For information about...	See topic...
You can specify a default value for user/group fields	“Defining fields and adding them to field groups” on page 161
You can use a hyphen (-) in field and field group names	“Defining field groups” on page 160 “Defining fields and adding them to field groups” on page 161
You can use a period (.) in object instance names	Rules for naming objects
You can disable past reporting periods. You can also re-enable them.	“Disabling finalized reporting periods” on page 459
You can define the Maximum Page Size setting to limit the number of resources on a page that a UI endpoint can request.	“Maximum page size” on page 500

Solution enhancements

See the *IBM OpenPages with Watson Solutions Guide* for a complete list of all the changes to solutions.

Table 6. Solution enhancements	
For information about...	See topic...
You can change the settings that are used for assessments in the Operational Risk Management solution	“Changing the settings for assessments in IBM OpenPages Operational Risk Management” on page 949

Administration and serviceability enhancements

Table 7. Administration and serviceability enhancements	
For information about...	See topic...
The ability to log HTTP requests to the IBM Watson® Language Translator service by using Applications > Watson Language Translator > Watson SDK Logging	“Configure HTTP request logging for IBM Watson Language Translator” on page 498
The <code>url.path.openpages</code> property in the <code>Server<#>-server.properties</code> is no longer used.	“OpenPages server properties and parameters” on page 933
You can now edit and create email notification templates within the Workflow Designer and assign templates to workflow stages.	“Defining a workflow action” on page 407 “Defining an end stage” on page 402 “Customizing email notification templates in workflows” on page 427

Table 7. Administration and serviceability enhancements (continued)

For information about...	See topic...
When you edit Microsoft Office files directly from OpenPages, the View button is no longer displayed by default and the file is now checked out as soon as the user clicks the Edit button. These are the recommended defaults, but you can decide to change them to preserve the behavior of previous versions.	“Enabling and configuring the opening of Microsoft Office files” on page 488
You can use the content assist feature to help you build an expression.	“Expressions in GRC Calculations” on page 342
You can export and import tags using FastMap.	“Exporting and importing tags with FastMap” on page 798
The Watson Machine Learning Integration has a new name: Custom Machine Learning Model Integration. The Custom Machine Learning Model Integration now supports connecting to Natural Language Understanding on IBM® Cloud for custom classification models.	“Setting up a connection to your model” on page 859

New and changed features in version 8.3.0.1

New and changed features in version 8.3.0.1 are described in the following tables.

For more information, see the *IBM OpenPages with Watson New Features Guide*.

Platform enhancements

Table 8. Platform enhancements

For information about...	See topic...
Integration with AI models	“Custom Machine Learning Models” on page 857
Creating an object based on scores in a questionnaire assessment	“Creating objects based on scores in a questionnaire assessment” on page 429
The new application permissions: <ul style="list-style-type: none">• Tagging• RapidRatings• RiskRecon Feed	“Types of application permissions” on page 52
Adding a trend chart with fields to a Task or Admin View to display the trends of numeric fields over time	“Adding a trend chart based on field value change history” on page 279

Solution enhancements

See the *IBM OpenPages with Watson Solutions Guide* for a complete list of all the changes to solutions.

Table 9. Solution enhancements	
For information about...	See topic...
OpenPages Third Party Risk Management includes a new connector to import data from RapidRatings	“RapidRatings connector for IBM OpenPages Third Party Risk Management” on page 921
OpenPages Third Party Risk Management includes a new connector to import data from RiskRecon	“RiskRecon connector for IBM OpenPages Third Party Risk Management” on page 922
The Ascent connector for IBM OpenPages Regulatory Compliance Management can now import Supporting Information	“Ascent Connector” on page 893

Administration and serviceability enhancements

Table 10. Administration and serviceability enhancements	
For information about...	See topic...
Keyboard navigation has been improved for workflows.	

New and changed features in version 8.3.0

New and changed features in version 8.3.0 are described in the following tables.

For more information, see the *IBM OpenPages with Watson New Features Guide*.

Platform enhancements

Table 11. Platform enhancements	
For information about...	See topic...
Reporting framework generation enhancements and changes including: <ul style="list-style-type: none">• A simpler user interface for generating the reporting framework• New out-of-the-box DQM framework models and namespaces	Chapter 29, “Configuring and generating the reporting framework,” on page 799
The name of the folder in IBM Cognos Analytics where platform reports are stored has changed. In fresh installations of OpenPages, reports and report pages are in Team Content > OpenPages Platform Reports .	
The platform reports have been updated: <ul style="list-style-type: none">• The reports now use the new Dynamic Query Mode (DQM) framework models.• The reports now use a new stylesheet to align more closely with the OpenPages user interface.• The reports use updated JavaScript for CrossTrack links.	<i>IBM OpenPages with Watson Report Author’s Guide</i>

Table 11. Platform enhancements (continued)

For information about...	See topic...
The new application permissions: <ul style="list-style-type: none">• Logs• RiskLens Feed• Watson Mapping and Taxonomy Suggestions• Publishing permissions	“Types of application permissions” on page 52 “Application permissions not contained under the SOX heading” on page 58
The Administration > Background Process > Get Process Info application permission now also gives access to the  > Other > Background Processes menu item	“Application permissions not contained under the SOX heading” on page 58
The maximum value of the Applications > Common > Administration > User Provisioning > Default User Password Expiration setting is now 9999. Previously, it was 99.	“Default User Password Expiration” on page 481
Email-related registry settings removed and replaced.	“Email registry settings” on page 963
The new setting Platform > Scheduler > > Default Transaction Timeout to specify the default timeout for scheduled jobs.	“Managing jobs ” on page 435
The new setting Platform > Processes > <Custom_job_name> > Transaction timeout to specify the timeout for custom jobs in the Scheduler.	“Implementing a Java class for custom jobs ” on page 440
In previous releases, the LogCollector functionality was available only as a command line utility. The LogCollector functionality is now available from the OpenPages user interface.	“Gathering logs with the LogCollector user interface” on page 693
The Signature Revoke workflow was added.	
The Home page now displays information about your last successful login and prior unsuccessful login attempts.	

Solution enhancements

This release includes many enhancements to the solutions. See the *IBM OpenPages with Watson Solutions Guide* for a complete list of the changes.

Administration and serviceability enhancements

Table 12. Administration and serviceability enhancements

For information about...	See topic...
The following settings in <code>aurora.properties</code> are deprecated and will be removed in a future release. If you have custom code (such as triggers, JSPs, etc.) that uses these settings, plan to update your custom code. <code>aurora.appserver</code> <code>aurora.initialcontext.factory</code> <code>server.use.local.ejb</code> <code>jta.initialcontext.factory</code> <code>jta.jndi.transaction</code> <code>javax.transaction.UserTransaction</code> <code>jms.initialcontext.factory</code> <code>workmanager.jndi.name</code> <code>workmanager.impl.classname</code>	“Aurora properties and parameters” on page 931
The <code>cognos.framework.refresh.servlet</code> property was removed from <code>aurora.properties</code> . The property is no longer used.	“Aurora properties and parameters” on page 931
Properties that are no longer used were removed from the <code><server_name>Server</#>-server.properties</code> file.	“OpenPages server properties and parameters” on page 933
Properties that are no longer used were removed from the <code><server_name>Server</#>-sosa.properties</code> file.	“Sosa properties and parameters ” on page 934
Properties that are no longer used were removed from the <code>objectmanager.properties</code> file.	“Settings in the ObjectManager.properties file ” on page 743
ObjectManager has changed.	“ObjectManager command line parameters” on page 733
The name of the White-listed Suspicious Character Combinations setting has changed. The new name is Allowed Suspicious Character Combinations .	“Configure allowed character combinations for URLs” on page 513
Some application permissions are no longer used.	“Legacy application permissions” on page 964
Some settings are no longer used and have been removed.	“Legacy registry settings” on page 963

Task Focused UI

This release includes several enhancements to the Task Focused UI.

The Standard UI is no longer available. See [“Removal of the Standard UI and other changes” on page 17](#).

Table 13. Task Focused UI enhancements

For information about...	See topic...
Admin Views were added and users can upgrade their Detail Views to Admin Views.	<p>“Admin Views” on page 252</p> <p>For more information about upgrading Detail Views to Admin Views, see <i>Upgrading Detail Views to Admin Views in the IBM OpenPages with Watson Installation and Deployment Guide</i>.</p>
Computed fields can now be defined in the Task Focused UI.	“Creating computed fields ” on page 181
Field exclusions on object types can now be defined in the Task Focused UI.	“Excluding fields from a subsystem” on page 216
Cognos reports can now be published automatically. The Add Cognos report button was added to  > System Configuration > Pages and Templates .	“Method 2: Automatically publishing Cognos reports” on page 138
Reporting fragment fields can now be defined in the Task Focused UI.	“Configuring reporting fragment fields” on page 176
Global search is now available. The results for Global Search might be different than in previous releases. OpenPages 8.3 includes a new version of the global search service (Solr). The new version of Solr ranks search result better.	Chapter 21, “Configuring the global search feature,” on page 517
The ability to view the status of background processes	Click  > Other > Background Processes .

Removal of the Standard UI and other changes

Version 8.3 includes the Task Focused UI only. Features and functions that were used only in the Standard UI are no longer available in fresh installations.

Several features from the Standard UI are now available in the Task Focused UI. See [“Task Focused UI” on page 16](#).

This release also removes other features that are no longer available in fresh installations.

Table 14. Standard UI features and functions removed

Feature or function	Notes
Filtered list views, folder views, detail views, and other Standard UI views are no longer supported.	For information about views, see Chapter 14, “Views,” on page 247 .
The syntax for creating links to views has changed. If you have links to Standard UI views, you need to update them..	See “Task-oriented hyperlinking” on page 954 .
The Switch To Standard UI menu command has been removed.	
Natural Language Classifier was removed and replaced	You can use IBM Watson Natural Language Understanding instead. See “Natural language processing services ” on page 850
Active reporting periods were removed.	

Table 14. Standard UI features and functions removed (continued)

Feature or function	Notes
Facts and dimensions were removed. In an upgrade or migration environment, any existing reports that rely on facts and dimensions will not work in 8.3.	Dimensional models are not supported. You can still define and generate recursive object levels in the relational framework. For more information, see the <i>IBM OpenPages with Watson Report Author's Guide</i>
The Approval app was removed.	You can use workflows and views instead.
The Code Cogs Equation Editor was removed.	This editor is no longer used.
VizConfig and Multiconnection were removed.	These items are no longer used.
Custom security was removed. The  > Users and Security > Custom Security menu item was removed as well as the functionality.	For information about security, see Chapter 6, "Security," on page 67 .
Custom forms were removed	Consider using questionnaires instead of custom forms. For more information, see <i>Questionnaires</i> in the <i>IBM OpenPages with Watson User Guide</i> .
The Relationship Type field (reference and association) in the object type properties was removed. Object relationships are now only association.	
The following object types are no longer included in fresh installations: <ul style="list-style-type: none"> • Quest • QSection • Questionnaire 	You can use the new questionnaires feature. See Chapter 31, "Configuring questionnaire assessments," on page 829
The following platform reports are no longer included in fresh installations: <ul style="list-style-type: none"> • Process Log Report • Process Log Report Detail All Statuses • Process Log Report Detail by Status • Process Log Report Full Detail 	These reports were used in the Standard UI only.
Header-based single sign-on is not supported	You SAML, OIDC, and SPNEGO single sign-on.
The Save as Draft feature is not supported	You can use workflows and views instead.
The Single File data type is no longer available.	For information about data types, see "Data types" on page 155 .
In the Standard UI, the Detail View had a Print button that enabled a user to get access to a print-friendly version of the Detail View. This feature is not available in the Task Focused UI.	

New and changed features in version 8.2.0.4

New and changed features in version 8.2.0.4 are described in the following tables.

For more information, see the *IBM OpenPages with Watson New Features Guide*.

IBM OpenPages for IBM Cloud Pak for Data

For more information, see [Chapter 3, “Administering IBM OpenPages for IBM Cloud Pak for Data,” on page 33.](#)

Platform enhancements

Table 15. Platform enhancements	
For information about...	See topic...
The > Watson Integrations menu was renamed. It is now called > Integrations	Chapter 33, “Configuring IBM Watson Integrations,” on page 843
The > Reporting Periods > Reporting Periods menu item is now > System Configuration > Reporting Periods	Chapter 19, “Reporting periods, object resets, and rulesets,” on page 457
The > Reporting Periods > Object Resets menu item is now > System Configuration > Object Resets .	Chapter 19, “Reporting periods, object resets, and rulesets,” on page 457
The > System Configuration > NPS Settings menu item is now > Integrations > NPS Settings .	“Configuring a Net Promoter Score survey” on page 239
The impact of the hyphen character (-) in display name format strings for user names has changed.	“Modifying how the names of users are displayed” on page 450
The ability to enable or disable reports for profiles.	“Adding reports to a profile” on page 227
Integrating an IBM Watson Natural Language Understanding classifier into OpenPages	“Natural language processing services ” on page 850
The Applications > GRCM > Object Move > Allow Hierarchical Moves setting now also controls rename operations	“Bulk move and rename setting” on page 497

Administration and serviceability enhancements

Table 16. Administration and serviceability enhancements	
For information about...	See topic...
Logging with Apache Log4j 2	“OpenPages with Watson standard log files” on page 696
The <code>ObjectManagerLogging.properties</code> file has been removed. The logging for ObjectManager is now defined in the client tools' <code>log4j2.properties</code> file.	“OpenPages with Watson standard log files” on page 696
Generating the reporting schema and framework by using the <code>RpsRpf</code> command line tool	“Generating the reporting schema and framework from a command line” on page 121

New and changed features in version 8.2.0.3

New and changed features in version 8.2.0.3 are described in the following tables.

For more information, see the *IBM OpenPages with Watson New Features Guide*.

IBM OpenPages for IBM Cloud Pak for Data

For more information, see [Chapter 3, “Administering IBM OpenPages for IBM Cloud Pak for Data,” on page 33](#).

Platform enhancements

Table 17. Platform enhancements	
For information about...	See topic...
The new API Version field on the configuration page for IBM Watson Language Translator	“Configuring the integration between IBM Watson Language Translator and OpenPages” on page 849
The new application permission: Bulk Update All Fields	“Types of application permissions” on page 52

Solution enhancements

See the *IBM OpenPages with Watson Solutions Guide* for a complete list of all the changes to solutions.

Table 18. Solution enhancements	
For information about...	See topic...
OpenPages Third Party Risk Management includes a new connector to import data from Supply Wisdom	“Supply Wisdom connector” on page 920
The new application permission: SupplyWisdom Feed	“Types of application permissions” on page 52

Administration and serviceability enhancements

Table 19. Administration and serviceability enhancements	
For information about...	See topic...
New application permissions for FastMap in the Task Focused UI	“Types of application permissions” on page 52

Task Focused UI

Table 20. Task Focused UI enhancements	
For information about...	See topic...
The ability to search for fields in Creation Views, Task Views, and Quick Views.	“Designing a Creation View” on page 260 , “Designing a Task View” on page 265
The FastMap import process	“The FastMap import process” on page 768 , “Accessing FastMap to import data and view status” on page 770

Table 20. Task Focused UI enhancements (continued)

For information about...	See topic...
The menu item for defining classifiers has changed to  > Watson Integrations > Mapping and Taxonomy Suggestions . It was previously named Administration > Cognitive Services > Natural Language Classifiers .	“Defining a classifier configuration” on page 854
IBM Watson Discovery was added as a natural language processing service.	“Natural language processing services ” on page 850 “Configuring Watson Discovery ” on page 853
The fields that are allowed to be updated by using Bulk Update () in Grid Views can now be configured.	“Designing a Grid View” on page 256 “Defining a Grid View” on page 257
It is now easier to create new views from existing ones. When creating new views in the View Designer, Copy from view (Optional) now allows you to copy from any existing published custom or system view (for the view type and object type).	“Defining a Creation View” on page 263 “Defining a Grid View” on page 257 “Defining a Task View” on page 268
Labels for existing fields can now be edited directly on the field definition.	“Defining fields and adding them to field groups” on page 161
Object type associations can now be enabled and disabled by using  > Solution Configuration > Objects Types .	“Enabling associations between object types” on page 200 “Disabling associations between object types” on page 200
The  > Solution Configuration > Objects menu item was renamed to  > Solution Configuration > Object Types .	
Reports can now be added to profiles. Users can now define report tabs on their dashboard. Previously, report tabs could be created only by administrators by using the Manage Dashboards task in the Task Focused UI.	“Adding reports to a profile” on page 227

GRC Workflow

Table 21. GRC Workflow enhancements

For information about...	See topic...
Calculations can now be started directly from a workflow action. <ul style="list-style-type: none">• Added Calculation Type to calculation definitions. Valid values are Automatic or Manual. Manual calculations are started only by a run a calculation action in a workflow.• Added the new run a calculation action to workflow stages.	“Defining a calculation” on page 338 “Defining a workflow action that runs a calculation” on page 425

New and changed features in version 8.2.0.2

New and changed features in version 8.2.0.2 are described in the following tables.

For more information, see the *IBM OpenPages with Watson New Features Guide*.

IBM OpenPages for IBM Cloud Pak for Data

For more information, see [Chapter 3, “Administering IBM OpenPages for IBM Cloud Pak for Data,” on page 33](#).

Platform enhancements

Table 22. Platform enhancements	
For information about...	See topic...
The default value for the user name format application text (com.display.name.format) was changed to %FN; %LN; - %EM (first name, last name, email).	“Modifying how the names of users are displayed” on page 450
The new setting Applications > GRCM > Allow Hierarchical Moves , which is set to false by default.	Controls whether child objects are moved with their parent objects by using the  icon in Grid Views: “Bulk move and rename setting” on page 497

Solution enhancements

See the *IBM OpenPages with Watson Solutions Guide* for a complete list of all the changes to solutions.

Table 23. Solution enhancements	
For information about...	See topic...
Configuring IBM OpenPages Data Privacy Management	Chapter 34, “IBM OpenPages Data Privacy Management,” on page 877
When you regulatory library data from Thomson Reuters into IBM OpenPages Regulatory Compliance Management, mandates are now created.	“Thomson Reuters Connector” on page 895

Administration and serviceability enhancements

Table 24. Administration and serviceability enhancements	
For information about...	See topic...
Improved logging for SAML, OIDC, and SPNEGO single sign-on	“Enabling trace logging” on page 698

Table 24. Administration and serviceability enhancements (continued)

For information about...	See topic...
<p>Name changes</p> <p>Note the following changes:</p> <ul style="list-style-type: none"> • bcprov-jdk14-145.jar is now bcprov-jdk15to18-1.68.jar • org.bouncycastle145.jce.provider.BouncyCastleProvider is now org.bouncycastle.jce.provider.BouncyCastleProvider • CAMCryptoBC is now BC 	
<p>Access to system files in the /Reports folder has changed. By default, only super administrators and members of the OPAdministrator group can now create or modify the JSP report system files in the /Reports folder under  > System Configuration > System Files.</p>	<p>“Adding and modifying system files” on page 150</p>

Task Focused UI

Table 25. Task Focused UI enhancements

For information about...	See topic...
<p>Defining themes.</p>	<p>“Themes” on page 241</p> <p>“Types of application permissions” on page 52</p>
<p>Colors are now based on two Carbon color palettes, Categorical and Monochromatic.</p>	<p>“Supported color palettes for field values” on page 159</p>
<p>Applying a color palette when configuring enumerated fields in the View Designer.</p>	<p>“Defining enumerated string fields” on page 170</p>
<p>Applying a color palette when configuring charts in the View Designer.</p>	<p>“Adding a chart diagram” on page 294</p>
<p>Organizing relationship fields in tab groups in the View Designer.</p>	<p>“Organizing relationship fields in tab groups” on page 312</p>
<p>Improved usability for disassociating objects. Added a Remove button to grid relationship fields that have an Associate action.</p>	<p>“Adding an Add action” on page 313</p>
<p>The new Field Groups section in the  > Solution Configuration > Objects task is used to work with field groups.</p>	<p>“Adding existing field groups to object types” on page 160</p>
<p>The new Field Dependencies section in the  > Solution Configuration > Objects task is used to work with field dependencies.</p>	<p>“Adding and working with dependent fields” on page 212</p>
<p>The new Dependent Picklists section in the  > Solution Configuration > Objects task is used to work with dependent picklists.</p>	<p>“Adding and working with dependent picklists” on page 214</p>

Table 25. Task Focused UI enhancements (continued)	
For information about...	See topic...
The environment migration tools are now available. Click  > System Migration > Export Configuration and  > System Migration > Import Configuration .	<p>“Exporting configuration items from the source environment” on page 727</p> <p>“Importing a migration file ” on page 729</p>

GRC Workflow

Table 26. GRC Workflow enhancements	
For information about...	See topic...
Email reminders can now be configured on standard stages in GRC Workflow.	“Defining a standard stage” on page 397
Users can now complete their workflow tasks in bulk. <ul style="list-style-type: none"> Added Bulk Workflow Action to standard stages. Added functionality to Grid Views to support bulk workflow actions. Added Complete tasks with bulk workflow actions window to My Tasks tab and panel, Subscription Tasks tab and panel, and Oversight Tasks tab and panel. 	“Defining a standard stage” on page 397 “Defining Grid Views for bulk workflow actions” on page 259 “How users interact with workflows ” on page 373
Added Override workflow action text to workflow actions. Use it to customize the text on the confirmation window that is displayed when users select a workflow action.	“Confirm the selected action” on page 375 “Defining a workflow action” on page 407

New and changed features in version 8.2.0.1

New and changed features in version 8.2.0.1 are described in the following tables.

For more information, see the *IBM OpenPages with Watson New Features Guide*.

IBM OpenPages for IBM Cloud Pak for Data

OpenPages can now be installed on IBM OpenPages for IBM Cloud Pak for Data. For more information, see [Chapter 3, “Administering IBM OpenPages for IBM Cloud Pak for Data,” on page 33](#).

Platform enhancements

Table 27. Platform enhancements	
For information about...	See topic...
New application permissions for the following features: <ul style="list-style-type: none"> Watson Language Translator NPS® Settings Reg-Track Connector 	“Types of application permissions” on page 52

Table 27. Platform enhancements (continued)

For information about...	See topic...
The new Applications > Common > Administration > System Files > Show GRC Folder Structure setting controls whether files for self-contained object types display under system files.	“Configure self-contained object types” on page 501
The new Applications > GRCM > Filtered List > Bulk Update Disabled in Task Focused UI settings controls whether the Bulk Update link displays in Grid Views in the Task Focused UI.	“Disable Bulk Update link” on page 496

Solution enhancements

See the *IBM OpenPages with Watson Solutions Guide* for a complete list of all the changes to solutions.

Table 28. Solution enhancements

For information about...	See topic...
IBM OpenPages Regulatory Compliance Management includes a new connector to import data from Reg-Track	“Reg-Track connector” on page 901

Administration and serviceability enhancements

Table 29. Administration and serviceability enhancements

For information about...	See topic...
The following new parameter for the LogCollector tool: --location	“Gathering logs with the log collector tool” on page 694
Installing tools and utilities, such as ObjectManager, on remote systems	“Installing tools and utilities (IBM OpenPages with Watson)” on page 692

Task Focused UI

Table 30. Task Focused UI enhancements

For information about...	See topic...
The new Watson Integrations > Watson Language Translator task on the Administration menu is used to integrate a Watson Language Translator service with OpenPages.	“IBM Watson Language Translator” on page 847
A Net Promoter Score (NPS) survey can now be displayed and submitted directly from OpenPages.	“Configuring a Net Promoter Score survey” on page 239
Microsoft Office files can now be opened and edited directly from OpenPages.	“Enabling and configuring the opening of Microsoft Office files” on page 488
The new  Solution Configuration > Objects task on the Administration menu is used to work with object types and supporting information.	“Working with object types” on page 198

Table 30. Task Focused UI enhancements (continued)

For information about...	See topic...
The definition of fields and field groups is included in the  > Solution Configuration > Objects task.	Chapter 10, “Fields and field groups,” on page 153 “Defining field groups” on page 160 “Defining fields and adding them to field groups” on page 161
The definition of public filters is included in the  > Solution Configuration > Objects task.	“Adding filters to object types” on page 208
Two new data types, Business Entity Selector and User Group, are available on fields. The Display Type attribute is now defined on fields in the Task Focused UI. It is still defined on profiles in the Standard UI.	“Data types” on page 155 Chapter 10, “Fields and field groups,” on page 153 “Defining fields and adding them to field groups” on page 161
The new  > Solution Configuration > Profiles task on the Administration menu is used to define profiles.	“Creating a profile ” on page 220
The new  > Users and Security > Domains & Groups task on the Administration menu is used to define domains and groups.	“Creating an organizational group ” on page 51 “Assigning and removing a role from a user or group ” on page 78
The new  > Users and Security > Role Templates task on the Administration menu is used to provision and modify role templates.	“Adding a role template ” on page 76
The new  > Users and Security > Security Rules task on the Administration menu is used to define security rules.	“Security rules” on page 80
Safe mode can now be applied to Dashboards.	“Defining a dashboard for a profile” on page 231

GRC Workflow

Table 31. GRC Workflow enhancements

For information about...	See topic...
Added Ancestor and Descendent as valid values in Relationship Type when choosing a field on a related object in the following places: <ul style="list-style-type: none">• Assign To and Adjust Date By on the Overall Due Date field on workflow properties.• Assign To and Due Date on the Due Date field on standard stages.• Add Assignee and Add Subscriber fields on standard stages.• Add User in End Stage Notifications fields on end stages.	“Defining workflow properties ” on page 392 “Defining a standard stage” on page 397 “Defining an end stage” on page 402

New and changed features in version 8.2.0

New and changed features in version 8.2.0 are described in the following tables.

For more information, see the *IBM OpenPages with Watson New Features Guide*.

Platform enhancements

Table 32. Platform enhancements	
For information about...	See topic...
The GRC Calculations feature.	Chapter 15, “Configuring GRC Calculations,” on page 327
The Scheduler feature.	Chapter 17, “Scheduler,” on page 435
The ability to run a GRC Workflow on a schedule.	“Defining workflow properties ” on page 392
The redesigned login page and how you can add a link to an acceptable use policy.	“Defining messages and behavior on the login screens” on page 451
The ability to add a privacy menu item and an acceptable use policy menu item to the Help menu.	“Defining the Privacy and Acceptable Use menu items” on page 476
The new configuration file, <code>openpages-tools-client.properties</code> .	“Tools properties and parameters ” on page 934
New application permissions for the following features: <ul style="list-style-type: none">• GRC Calculations• Scheduler• IBM Watson Assistant (separate application permissions for administrators and users)• Notification Manager• ObjectManager• Administration menu items in the Task Focused UI	“Types of application permissions” on page 52
The Audit Trail (Change History) application permission also applies to the new Activity tab in Task Views.	“Types of application permissions” on page 52 “Task Views” on page 251
Functionality that supported the integration of IBM OpenPages with Watson with IBM Business Process Manager was removed.	
Visualizations that rendered business processes in a graphical format are no longer supported.	
By default, you can now create QuestionnaireAssessments with the Add New wizard. The default value of Applications > GRCM > Add New Wizard > Object Types Disabled has changed. It no longer includes QuestionnaireAssessments.	“Controlling the availability of object types with the New button on Grid Views” on page 213

Solution enhancements

See the *IBM OpenPages with Watson Solutions Guide* for a complete list of all the changes to solutions.

Table 33. Solution enhancements	
For information about...	See topic...
The new setting for Wolters Kluwer data feeds: Solutions > RCM > WK > Max Days To Get	“Data import settings for Wolters Kluwer feeds” on page 908
The new connector that enables you to import obligations from Ascent Reg Tech feeds	“Ascent Connector” on page 893

Administration and serviceability enhancements

Table 34. Administration and serviceability enhancements	
For information about...	See topic...
Properties that are no longer used were removed from the <code>aurora.properties</code> file.	“Aurora properties and parameters” on page 931
Properties that are no longer used were removed from the <code><server_name>Server</#>-server.properties</code> file.	“OpenPages server properties and parameters” on page 933
Properties that are no longer used were removed from the <code><server_name>Server</#>-sosa.properties</code> file.	“Sosa properties and parameters ” on page 934
Properties that are no longer used were removed from the <code>objectManager.properties</code> file.	“Settings in the ObjectManager.properties file ” on page 743
ObjectManager has changed. <ul style="list-style-type: none">• The <code>ObjectManager.log</code> file is now created in the directory that you specify in the <code><loader-file-path></code> parameter. If the parameter is not specified, the log file is created in the current directory.• The <code>-server</code> parameter is ignored because ObjectManager now runs on the server.• New application permissions are used.	“ObjectManager command line parameters” on page 733
The <code>JSON4J_Apache.jar</code> file is deprecated.	
The default protocol that is used by OpenPages for secure connections (SSL/TLS) is now TLSv1.2.	
You can now install and run the following tools and utilities on a remote system: <ul style="list-style-type: none">• ObjectManager• Update Password Encryption Algorithm (UPEA)• <code>chng-sys-password.sh bat</code>• <code>RpsRpf.sh bat</code>• Notification Manager	“Installing tools and utilities (IBM OpenPages with Watson)” on page 692

Task Focused UI

Table 35. Task Focused UI enhancements

For information about...	See topic...
The Settings menu was renamed to the Administration menu. It is now organized into categories.	
The new Calculations task on the Administration menu is used to manage calculations.	Chapter 15, “Configuring GRC Calculations,” on page 327
The new Scheduler task on the Administration menu is used to manage jobs.	Chapter 17, “Scheduler,” on page 435
The new Solutions task on the Administration menu is used to manage solution schema visualizations.	“Solution schema visualizations ” on page 195
The new  > Users and Security > Users task on the Administration menu is used to provision and modify users.	“Creating user accounts ” on page 48
The new  > Users and Security > User LDAP Configuration task on the Administration menu is used to define LDAP for user provisioning.	“Configuring LDAP access for user provisioning ” on page 47
The new  > Users and Security > Custom Security task on the Administration menu is used to define security access for Project Milestones and Project Action Items.	
The new  > Users and Security > Encryption Keystore task on the Administration menu is used to configure the encryption keystore.	“Setting up the encryption keystore” on page 105
The new  > System Configuration > System Files task on the Administration menu is used to add and manage system files and folders.	Chapter 9, “System file management,” on page 145
The new  > Watson Integrations > Watson Assistant task on the Administration menu is used to integrate an assistant with OpenPages.	“Configuring the integration between an assistant and OpenPages ” on page 844
Classifier fields are now displayed using an IBM Watson Insights button and panel.	“Natural language processing services ” on page 850
The new  > Watson Integrations > Natural Language Classifiers task on the Administration menu is used to define a classifier configuration.	“Defining a classifier configuration” on page 854
The reporting framework can be generated using the new Reporting Framework Generation task on the Administration menu.	“Updating the reporting framework” on page 817
Details about reporting framework generation operations can be viewed using the new Reporting Framework Generation task on the Administration menu.	“Viewing reporting framework details” on page 817

Table 35. Task Focused UI enhancements (continued)

For information about...	See topic...
Currency exchange rates can be modified and uploaded using the new Currencies task on the Administration menu.	“Editing, enabling, disabling, and uploading currency exchange rates” on page 168
The reporting schema can be modified using the new Reporting Schema task on the Administration menu.	“Creating or re-creating the reporting schema” on page 120
Reporting periods can be created, finalized, and deleted using the new Reporting Periods task on the Administration menu.	“Creating a finalized a reporting period” on page 458
Object resets can be started using the new Object Resets task on the Administration menu.	“Starting the object reset” on page 469
System Admin Mode can be enabled and disabled from the Task Focused UI.	“Enabling and disabling System Admin Mode” on page 37
Light formatting can now be applied to object text.	“Modifying object text” on page 445
New Gantt charts in chart relationship fields in Task Views and on Dashboards.	“Adding a chart diagram” on page 294
New method type and aggregation field for sum, average, min, and max on charts in Task Views and Dashboards.	“Adding a chart diagram” on page 294
A delete action can now be added to grid relationship fields in Task Views.	“Adding a Delete action” on page 317
Multiple Grid Views can now be defined for an object type.	“Defining a Grid View” on page 257
Multiple Creation Views can now be defined for an object type.	“Defining a Creation View” on page 263
New rule type can determine what Creation View is displayed. The rule type is based on the parent object type, if it is known at creation time.	“Defining a Creation View” on page 263
A dashboard can now contain a Search panel.	See “Adding a Search panel” on page 232 for more information.
A grid relationship field for File object type can now contain an Associate action.	“Defining Task Views for file object types” on page 269
Creation Views for files can now use a File Uploader element.	“Defining Creation Views for file object types” on page 264

GRCA Workflow

Table 36. GRC Workflow enhancements

For information about...	See topic...
<p>In applicability, conditions, and validations that are based on a related object, added Relationship Type and Relationship Paths. This makes it easier to associate the related object.</p>	<p>“Defining workflow properties” on page 392</p> <p>“Defining an end stage” on page 402</p> <p>“Defining a workflow action” on page 407</p> <p>“Defining a workflow action that creates objects” on page 413</p> <p>“Defining a workflow action that runs a custom action” on page 415</p> <p>“Defining a workflow action that locks or unlocks objects” on page 417</p> <p>“Defining a workflow action that sets fields” on page 420</p> <p>“Defining a workflow action that starts a workflow” on page 422</p>
<p>Whether workflow information card content is automatically updated when object information changes is now controlled by a registry setting, Platform > Calculation > Refresh Workflow Information Automatically.</p>	<p>“How users interact with workflows” on page 373</p>
<p>The review process for questionnaire assessments can now be driven by GRC Workflow.</p>	<p>Chapter 31, “Configuring questionnaire assessments,” on page 829</p>
<p>Added Execute As System to workflow properties.</p>	<p>“Defining workflow properties” on page 392</p>
<p>Added Execute As System to create objects actions.</p>	<p>“Defining a workflow action that creates objects” on page 413</p>
<p>Added Execute As System to custom action.</p>	<p>“Defining a workflow action that runs a custom action” on page 415</p>
<p>Added Execute As System to lock or unlock objects.</p>	<p>“Defining a workflow action that locks or unlocks objects” on page 417</p>
<p>Added Execute As System to set fields.</p>	<p>“Defining a workflow action that sets fields” on page 420</p>
<p>Added Execute As System to start workflow.</p>	<p>“Defining a workflow action that starts a workflow” on page 422</p>

Chapter 3. Administering IBM OpenPages for IBM Cloud Pak for Data

IBM OpenPages for IBM Cloud Pak for Data is an integrated governance, risk, and compliance platform that companies can use as a tool to assist in managing risk and regulatory challenges across the enterprise.

It provides a set of core services and functional components that span risk and compliance domains, which include operational risk, policy management, financial controls management, IT governance, internal audit, model risk governance, regulatory compliance management, third-party risk management, and business continuity management.

IBM OpenPages for IBM Cloud Pak for Data provides a powerful, highly scalable, and dynamic tool set that helps empower managers with information transparency and the capability to identify, manage, monitor, and report on risk and compliance initiatives on an enterprise-wide scale.

Documentation for IBM OpenPages for IBM Cloud Pak for Data administrators

Some administrative tasks do not apply in IBM OpenPages for IBM Cloud Pak for Data. Use the following table to help you find the information that's relevant to IBM OpenPages for IBM Cloud Pak for Data.

For information about...	See
Files and directories	Files and directories in IBM OpenPages for IBM Cloud Pak for Data
Setting up users and groups	Managing users and groups within IBM OpenPages for IBM Cloud Pak for Data
<ul style="list-style-type: none">• Connecting to your LDAP server• Configuring SAML single sign-on	Managing users
Adding IBM Cognos Analytics to OpenPages instances	IBM Cognos Analytics and IBM OpenPages for IBM Cloud Pak for Data
Security	<ul style="list-style-type: none">• “Role-based security model” on page 67• “Security rules” on page 80
Setting up the object model (object types, profiles, fields, and field groups)	<ul style="list-style-type: none">• Chapter 11, “Object types,” on page 195• Chapter 12, “Profiles,” on page 219• Chapter 10, “Fields and field groups,” on page 153• Chapter 7, “Managing the reporting schema ,” on page 117
Configuring the home page and dashboards	“Home page, dashboard, and tabs” on page 230
Creating views	<ul style="list-style-type: none">• Chapter 13, “Configuring the UI,” on page 229• Chapter 14, “Views,” on page 247• “Using the View Designer” on page 272• Chapter 31, “Configuring questionnaire assessments,” on page 829

For information about...	See
Creating calculations	Chapter 15, “Configuring GRC Calculations,” on page 327
Designing and creating workflows	Chapter 16, “Configuring GRC Workflow ,” on page 369
Scheduling jobs	Chapter 17, “Scheduler,” on page 435
Localizing text in the application user interface	Chapter 18, “Localizing text,” on page 443
Importing and exporting data	<ul style="list-style-type: none"> • Chapter 28, “Using FastMap,” on page 767: A user interface for importing and exporting data • Chapter 27, “The ObjectManager tool,” on page 731: A command-line tool for importing and exporting data <p>To install ObjectManager, see Installing tools and utilities in Cloud Pak for Data.</p>
Environment configuration and system maintenance	<ul style="list-style-type: none"> • “Managing settings ” on page 473: Some settings do not apply in IBM OpenPages for IBM Cloud Pak for Data environments • Chapter 9, “System file management,” on page 145 • Appendix B, “Properties and parameters,” on page 931: Describes the properties and parameters in configuration files • “Auditing configuration changes” on page 634 • Installing tools and utilities in Cloud Pak for Data • Starting and stopping application servers in IBM OpenPages for IBM Cloud Pak for Data • Changing the password of the OPSystem user in Cloud Pak for Data • Changing the password of the Liberty keystore in IBM OpenPages for IBM Cloud Pak for Data • Logging in to the database in IBM Cloud Pak for Data
Configuring apps and integrations	<ul style="list-style-type: none"> • “IBM Watson Assistant ” on page 843 • “IBM Watson Language Translator” on page 847: You can integrate with a service instance that is hosted on IBM Cloud • IBM OpenPages SDI Connector for UCF Common Controls Hub: See the <i>IBM OpenPages with Watson Installation and Deployment Guide</i> • “Natural language processing services ” on page 850: You can integrate with IBM Watson Discovery on IBM Cloud Pak for Data or the Natural Language Classifier service on IBM Cloud • Chapter 32, “Configuring OpenPages Loss Event Entry,” on page 831
Configuring connectors for data feeds	<ul style="list-style-type: none"> • “Ascent Connector” on page 893 • Chapter 35, “IBM OpenPages IT Governance with RiskLens,” on page 881 • “RapidRatings connector for IBM OpenPages Third Party Risk Management” on page 921 • “RiskRecon connector for IBM OpenPages Third Party Risk Management” on page 922 • Chapter 36, “IBM OpenPages Model Risk Governance,” on page 885

For information about...	See
	<ul style="list-style-type: none"> • “Reg-Track connector” on page 901 • “Thomson Reuters Connector” on page 895 • “Wolters Kluwer Connector” on page 906 • “SecurityScorecard connector for IBM OpenPages Third Party Risk Management” on page 919 • “Supply Wisdom connector” on page 920
Best practices and troubleshooting	<ul style="list-style-type: none"> • Appendix D, “Best practices for configuring IBM OpenPages with Watson,” on page 953 • Appendix C, “Troubleshooting and support for IBM OpenPages with Watson,” on page 937

Chapter 4. System Admin Mode (SAM)

Use System Admin Mode (SAM) to restrict user access to the system when you apply configuration changes or other updates to the system.

When System Admin Mode (SAM) is enabled, the following conditions are enforced:

- Only administrative users with **System Administration Mode** application permission can log on to the system. All other users are restricted from logging on.
- All Write operations are restricted, with these exceptions:
 - Reporting period operations if the reporting schema is not enabled
 - Metadata (schema) changes
 - Enumerated string conversions from single to multivalued selection
 - Setting changes that are made through the user interface

Before you enable SAM, you may want to notify application users to log off the system. If a user is already logged on to the system when SAM is enabled, the user will only be able to view objects and will not be able to create new instances of objects or save any modifications made to existing objects.

Depending on your configuration, SAM mode might not start until all asynchronous background jobs run to completion. For more information, see [“Asynchronous background jobs and administrative functions” on page 547](#).

You must be in System Admin Mode (SAM) if you:

- Want to create, re-create, enable, or drop a reporting schema. For more information see, [Chapter 7, “Managing the reporting schema,” on page 117](#).
- Have an existing reporting schema and you want to add, remove, or refresh a reporting period.
- Have configuration changes to make to the system, such as changes to the object model hierarchy or modifications to object types, field groups, and object fields.
- Are converting an enumerated string value from a single selection to a multi-value selection. For more information, see [“Defining enumerated string fields” on page 170](#).
- Set up field level security.

In all other instances you can make configuration changes without enabling SAM. However, there may be situations where you want to enable SAM to restrict general user access. For example, if you need to modify one or more object text labels, you may not want users to create new instances of the object type while you are making these changes.

Enabling and disabling System Admin Mode

You can enable and disable System Admin Mode (SAM).

About this task

If the system is processing operations that require System Admin Mode, you must wait until processing is complete before you can disable System Admin Mode.

Procedure

1. Log on to IBM OpenPages with Watson as a user with the **System Administration Mode** permission.
2. To enable System Admin Mode, click  > **Enable System Admin Mode**.
3. To disable System Admin Mode, click  > **Disable System Admin Mode**.

Chapter 5. Users, groups, and domains

Access within the IBM OpenPages with Watson application is administered through the use of users, groups, and domains.

To create and administer users and groups, you must have administrative privileges.

- To access the  > **Users and Security** > **Users** menu item, you must have **Browse** permission on any security domain or any user group.
- To access the  > **Users and Security** > **Domains & Groups** menu item, you must be a Super Administrator or a delegated administrator with any administrator permission. For information about delegating and assigning administrator permissions, see [“Delegate administrator permissions” on page 42](#).
- For information about the administrative permissions that are required for specific user-provisioning functions, see [“Types of administrator permissions” on page 43](#).

Users and groups are organized under the following top-level groups:

- Security Domains

This group is a container for the security domain groups that are automatically created by the system when a business entity or sub-entity is added. You can use security domains to distribute your users and organizational groups so they can be administered by administrators with appropriate permissions. For an overview of security domains, see [“Security domains” on page 72](#).

When you expand a security domain group folder, only child security domains are displayed. To view the organizational groups and users that are associated with the security domain, click the security domain group.

- Workflow, Reporting and Others

This group is a container for organizational groups that are used system-wide. For example, the OPAdministrators group is listed under the special group **Workflow, Reporting and Others** > **Standalone Users and Groups**. The OPAdministrators group is created automatically at installation and members of the group are automatically granted special privileges.

Administrators often create organizational groups to organize users and other groups. You can define all your users and groups under the Workflow, Reporting and Others group, and later associate them to different security domains. For upgrade customers, this top-level group also includes the groups that existed in prior releases of OpenPages with Watson.

To navigate to a group's details page, you must be a super administrator or a delegated administrator of that group with at least **Browse** administrative permission. For information on delegating administrator permissions, see [“Delegate administrator permissions” on page 42](#).

Note: The term “group” includes both organizational and security domain groups, unless otherwise specified.

The OPAdministrators group

The OPAdministrators group is created automatically during the installation process. The group is listed under the special group **Workflow, Reporting and Others** > **Standalone Users and Groups**. Members of the OPAdministrators group are automatically granted special privileges.

Members of the OPAdministrators group can see the following items on the **Administration** menu:

- **System Files**
- **User LDAP Configuration**
- **Pages and Templates**

- **Cognos Integration** (on IBM Cloud Pak for Data)

Members of the OPAdministrators group are the only users that have Read, Write, Delete, and Mange permissions on the **Pages and Templates/Reporting** folder by default. Members of the OpenPagesApplicationUsers group have Read access. Individual features on the **Pages and Templates** page require different permissions. For more information, see “[Publishing permissions](#)” on page 59.

Members of the OPAdministrators group are the only users that have access to the following folders by default:

- The `/Migration Documents` folder, which is needed for environment migration.
- The `/LogCollector Documents` folder, which is needed for logging.

A user must be a member of the OPAdministrators group to perform the following user provisioning functions:

- Clearing direct reports access when you are disabling a user account.
- Viewing a user's reports access.
- Copying direct reports access from one user to a new or existing user.

More permissions might be required such as **Manage** permission on the top-level user group. For more information about the privileges you need to perform user provisioning functions, see “[Administrator permissions for user-provisioning functions](#)” on page 43.

Planning user administration

There are numerous things to consider before you create, modify, or copy a user account.

The following list outlines the tasks that you should perform before you begin creating, modifying, or copying users:

1. Determine whether you want to integrate IBM OpenPages with your LDAP servers to allow prepopulation of user information when you create a new user in IBM OpenPages. If so, then perform one or both of the following actions:
 - If you are using LDAP over SSL/TLS, [setup your certificates](#).
 - [Configure access to your LDAP servers](#) from IBM OpenPages.
2. Determine whether you want to allow the creation or updating of users based upon existing users. The user will have the same attributes, such as locale, profiles, group memberships, role assignments, and reports access, as another user. If so, then perform the following actions:
 - [Determine which users can be used as source for the Copy Access From operation](#).
 - [Determine whether you want to allow inactive users to be the source for the Copy Access From operation](#).
 - [Configure the default behavior for the Locale, Profiles, Group Memberships, Direct Role Assignments, and Direct Reports Access attributes during the Copy Access From operation](#).
 - [Determine whether the Copy Access From operation adds to or replaces a user or group's existing attributes](#).
3. Determine the default values for the following settings:
 - [The default value or values for the Allowed Profiles](#).
 - [The default value for the locale](#).
 - [The number of rows that are listed per page in the Reports Access table](#).
4. Determine the password behavior for users by performing the following actions:
 - [Configure the default change password behavior when you create a new user](#).
 - [Configure the default password expiration behavior](#).
5. If user provisioning is configured in your system to allow copying attributes from inactive users, determine whether you want to create template users as inactive users. The inactive template users

should have similar attributes that you want to copy to other users. The administrator can modify attributes after the copy operation.

6. Determine whether you want to add administrators who can perform user provisioning tasks beyond the super user. For example, you can create administrators who perform only password management tasks for users, while other administrators can create users.

Note: You must assign delegated administrators rights at the top-level security domain and the top-level user group to perform some user-provisioning functions. For more information, see [“Administrator permissions for user-provisioning functions” on page 43](#). For these functions, you can separate out the tasks the delegated administrators can do but cannot separate out which places they can perform them.

7. Determine whether you want to primarily manage administrative rights, such as managing profiles, role assignments, and reports access, directly at the user level or by making users members of user groups. You can use a combination of methods. It is strongly recommended that you manage administrator rights via user groups.
8. Determine the groups and security domains that you want each user to belong to. By default, when you create a new user from scratch, that user belongs to a special group called Standalone Users and Groups. Only the Super Administrator has administrative access to this group. When a user or group is disassociated from an organizational or security domain group, and that user or group is not a direct or indirect member of any other group, the system makes that user or group a member of Standalone Users and Groups.

For more information about group memberships, see [“Associating and disassociating a group” on page 51](#).

9. Determine the profiles that you want the users to have.

For more information about choosing profiles, see [Chapter 12, “Profiles,” on page 219](#).

10. Determine the role assignments that you want the user to have.

For more information about role-based security and role templates, see [“Role-based security model” on page 67](#).

11. Determine the reports that you want the users to have access to.

For more information about modifying reports access, see [Chapter 8, “Managing reports,” on page 125](#).

The Super Administrator

A Super Administrator is a user who has complete access to all objects, folders, role templates, and groups in the system. A deployment can have one or more Super Administrators.

- A Super Administrator can create users, groups, and other super administrators.
- A Super Administrator can delegate administration activities by assigning roles to users by using role templates and group administrator permissions. For more information about role templates, see [“Role templates” on page 75](#). For more information about group administrator permissions, see [“Delegate administrator permissions” on page 42](#).

For example, a Super Administrator can delegate user provisioning functions to other administrators. For more information, see [“Administrator permissions for user-provisioning functions” on page 43](#).

A Super Administrator is specified during the installation process. The Super Administrator user is a member of a group named OPAdministrators. For more information about the OPAdministrators group, see [“The OPAdministrators group” on page 39](#).

In a new installation, the Super Administrator is the only user in the system. In an upgrade, you can enter a new user or select one of the existing users as a Super Administrator.

Do not use the Super Administrator account for daily administrative actions. Create an administrator user ID for each of your administrators to allow for accountability within the system.

Creating a Super Administrator

If you are logged in to IBM OpenPages with Watson as a Super Administrator, you can create other super administrators.

You create a Super Administrator by adding Super Administrator status to an existing user account.

1. Click  > **Users and Security** > **Users** and select the user account that you want to modify.

For more information, see “[Modifying user accounts](#)” on page 49.

2. On the **User Information** page, set **Super Administrator** to true.

The field is grayed-out if:

- You are not logged in as a Super Administrator.
- You are modifying your own user account.

Tip: You can delegate administrator activities instead of (or in addition to) creating Super Administrators. See [“Role templates” on page 75](#) and [“Delegate administrator permissions” on page 42](#)

You can revoke Super Administrator status by setting **Super Administrator** to false. The field is grayed-out if:

- You are not logged in as a Super Administrator.
- You are modifying your own user account.
- Only one Super Administrator is configured. Each deployment must have at least one Super Administrator.

Delegate administrator permissions

By assigning specific security management permissions to an administrator's user account, you can delegate various security management activities to that administrator. For example, you could set up one administrator who would only have the ability to reset passwords for users, another who could lock and unlock users, and a third who could create users and associate them to user groups and assign them role templates.

For more information about entity groups, see [“Security context points” on page 69](#)). If there are child groups under a parent group, the administrator can delegate an administrator for each child group as well.

Administrators do not need to be members of groups for which they perform administrative tasks. By default, only the Super Administrator has Read and Write access to objects in the system. Delegating administration responsibilities to a user on a security domain, does not automatically grant Read and Write access to objects under the corresponding entity.

Important:

- You can assign to other administrators only the permissions that you have.
- If you disassociate an administrator from a security domain or organizational group, all user management privileges (such as manage users, lock/unlock users, reset passwords, enable/disable users, assign roles) are retained by that administrator and are not revoked.

Example

You want to designate Mary Smith as an administrator who can reset passwords for any users. You would assign the **Reset Password** permission to Mary Smith.

Note:

- When administrator permissions are assigned to a user, the name of that user is no longer displayed in the user selector list. To modify permissions for an administrator, see [“Assigning, modifying, and removing administrator permissions on groups” on page 45](#).
- Security domain groups are not displayed in the User/Group selector list.

Note: Administrators with **Settings** application permission can configure the behavior of some user-provisioning functions. For more information, see “User provisioning settings” on page 480.

Types of administrator permissions

There are six security management permissions that you can delegate to a security domain or user group administrator.

Table 37. Administrator permissions	
Permission	Description
Manage	Allows the delegated administrator to create, modify, and associate users and groups.
Lock	Allows the delegated administrator to lock a user account, which prevents logon to the IBM OpenPages with Watson application from that account. With this permission, a Lock User link can be clicked in the User Information section of a user account.
Unlock	Allows the delegated administrator to unlock a previously locked user account. With this permission, an Unlock User link can be clicked in the User Information section of a user account.
Reset Password	Allows the delegated administrator to reset passwords for users.
Assign Role	Allows the delegated administrator to assign one or more roles to users and groups and to revoke a role from a user or group. This permission applies to security domains only.
Browse	Allows the delegated administrator to view users and groups within that group. This permission is selected by default.

Administrator permissions for user-provisioning functions

You must have the appropriate administrator permissions to perform each user-provisioning function.

Table 38. Permissions required for user provisioning functions	
To do the following...	You must have these permissions...
View: <ul style="list-style-type: none">The  > Users and Security > Users menu item	Browse on any security domain or any user group.
View: <ul style="list-style-type: none">The Create User button from a list of users and create new users	Manage on any security domain or any user group. If LDAP Server integration is configured, there is an additional field that you can use to search for user in LDAP Server and prepopulate their user information. For more information, see “LDAP and user provisioning” on page 46.
Edit user information	Manage on any security domain or any user group that includes the user account.

Table 38. Permissions required for user provisioning functions (continued)

To do the following...	You must have these permissions...
Enable and disable user accounts	<p>Manage on any security domain or any user group that includes the user account.</p> <p>To clear direct role assignments when you disable a user account, you must have Assign Role on the root security domain.</p> <p>To clear group memberships when you disable a user account, you must have Manage on the top-level user group.</p> <p>To clear direct reports access when you disable a user account, you must belong to the OPAdministrators group.</p> <p>Note that an administrator cannot disable their own account.</p> <p>For information about the difference between disabling and locking user accounts, see “Modifying user accounts” on page 49.</p>
Lock user accounts	<p>Lock on any security domain or any user group that includes the user account.</p> <p>Note that an administrator cannot lock their own account.</p>
Unlock user accounts	Unlock on any security domain or any user group that includes the user account.
Edit user passwords This includes the Password and Confirm Password fields.	Reset Password on any security domain or any user group that includes the user account.
Configure password options and edit configured password options This includes the following options: User must change password at next log on , User cannot change password , Password never expires , Password expires in <n> days , and Force Password Change .	<p>Manage on any security domain or any user group that includes the user account.</p> <p>Note that an administrator can force a password change for their account and reset their password.</p>
Edit a user's locale and profile information	Manage on any security domain or any user group that includes the user account.
Modify a user's group memberships	Manage on the top-level user group.
Add role assignments to a user	Manage and Assign Role on the root security domain.
Remove role assignments from a user	Assign Role on the root security domain.
View a user's reports access	OPAdministrators group membership. Information is read-only.

Table 38. Permissions required for user provisioning functions (continued)

To do the following...	You must have these permissions...
Copy access from one user to a new or existing user This includes locale, profiles, group memberships, and direct role assignments.	Manage on the top-level user group and Manage and Assign Role on the root security domain.
Copy direct reports access from one user to a new or existing user	Manage on the top-level user group, Manage and Assign Role on the root security domain, and OPAdministrators group membership. Information is read-only.

Example

Figure 1 on page 45 shows a diagram with a sample security administration structure.

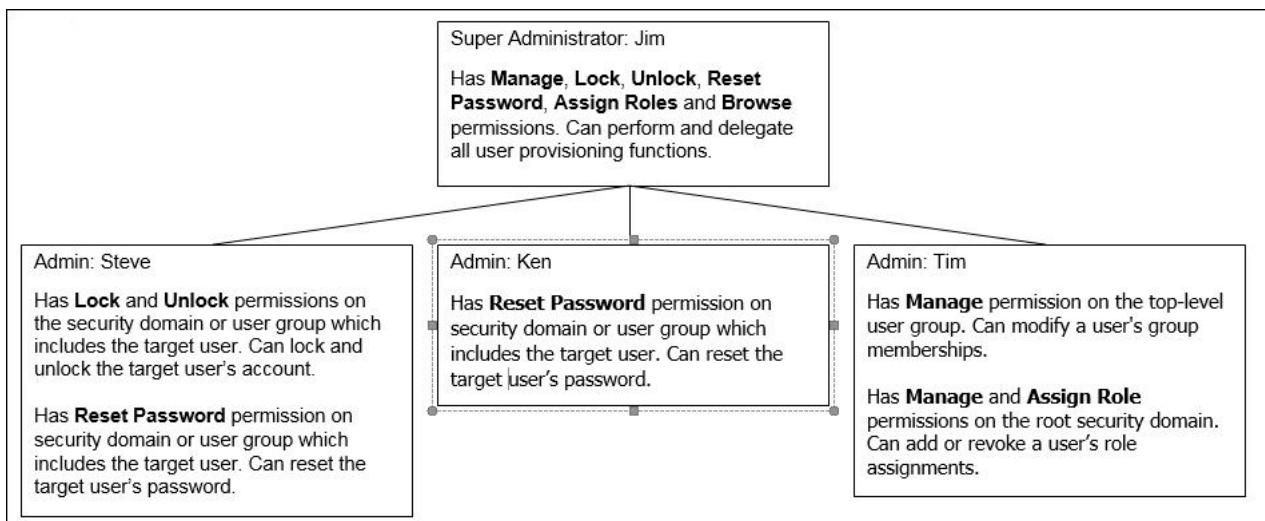


Figure 1. Sample security administration

Assigning, modifying, and removing administrator permissions on groups

You can assign one or more group administrator permissions to selected users. You can also modify and remove group administrator permissions.

About this task

A group contains the following sections:

- **Group Information**
- **Administrators & Permissions**
- **Groups**
- **Users**
- **Role Assignments**
- **Permissions**

Procedure

1. Click > **Users and Security** > **Domains & Groups**.
2. Click **Groups**.

3. Expand the folder structure to find the group you want to work with.
4. Click the name of the group for which you want to assign administrative permissions to selected users.
5. To assign administrator permissions, go to the **Administrators & Permissions** section.
 - a) Click **Add**.
 - b) Search for and select a user or group.
 - c) From the **Permissions** list, select the administrative permissions that you want to assign to this user (see “[Types of administrator permissions](#)” on page 43 for a list of permissions).
 - d) Click **Add**.
6. To remove a user or group's administrator permissions entirely, go to the **Administrators & Permissions** section.
 - a) From the list of administrative users, click the check box next to the user or group.
 - b) Click **Remove**.

LDAP and user provisioning

You can configure access to your LDAP server or servers from IBM OpenPages with Watson so that you can access user information from your LDAP server or servers when creating users in IBM OpenPages.

Through an LDAP server integration with IBM OpenPages, you can search your company's LDAP servers for a list of people who meet the search criteria. You can then select a user from the list and the information fields in the **Create User** page will be pre-populated with the user's information from the LDAP server.

Note: LDAP configuration for user provisioning does not affect LDAP user authentication.

Importing an LDAP certificate to the local truststore

If you are using LDAP over SSL/TLS, you must import an LDAP certificate to the local truststore before you can configure LDAP for user provisioning. It is needed to build a secure communication between the OpenPages with Watson servers and your LDAP over SSL/TLS server.

Before you begin

The target LDAP server from which you are going to retrieve the certificate must be running and listening on the port.

Procedure

1. Get the certificate from your LDAP server by using your browser or openssl.
2. Import the certificate by running this command:

```
keytool -importcert -v -alias <CERTIFICATE_ALIAS> -file <CERTIFICATE_NAME> -keystore <STORE_PATH> -storetype PKCS12 -storepass <STORE_PASSWORD>
```

Where:

- <CERTIFICATE_ALIAS> type an alias for the certificate.
- <CERTIFICATE_NAME> is the file name of the certificate.
- <STORE_PATH> is the full path and file name of the truststore on the application server. For example: <OP_HOME>/wlp-user/servers/<server_name>Server<#>/resources/security/key.p12
- <STORE_PASSWORD> is the password of the truststore on the application server.

For more information, see [Adding trusted certificates in Liberty](#) in the WebSphere Liberty documentation.

3. Restart the OpenPages with Watson application services.
4. Repeat these steps on each application server.

Configuring LDAP access for user provisioning

You can configure access to your LDAP server to import LDAP user information when you create users in IBM OpenPages with Watson.

Before you begin

To configure LDAP access for user provisioning, you must be a member of the OPAdministrators user group and have the following application permission; **All Permissions > SOX > Administration > LDAP Server.**

If you are using LDAP over SSL/TLS, complete the [preconfiguration task](#) first.

Procedure

1. Click  > **Users and Security > User LDAP Configuration.**
2. Click **New**.
3. Type a name for the LDAP configuration.

You can configure multiple LDAP servers. When you use multiple servers, the **Create User** page shows the search results from all LDAP servers. The maximum number of search results displayed on the page is the sum total of the maximum results configured for each LDAP server.

4. In the **Provider URL** field, type the LDAP service provider that you want to use.

The value must be a URL string, such as `ldap://<hostname>:389`.

Or, if you are using SSL/TLS: `ldaps://<hostname>:636`

Note: If you are using LDAP over SSL/TLS, you need to do some additional [preconfiguration steps](#).

5. Enter the values for your LDAP server. For information about a field, click the field.

Required fields have a red * next to the field name.

In the **First name attribute**, **Middle name attribute**, and **Last name attribute** fields, type the attribute names that you want to map to the OpenPages user's given name, middle name, and surname.

Note: The middle name is not displayed in OpenPages by default. You might want to display it so that you can differentiate users who have the same given name and surname. To display the middle name in the search results of the **Create User** page, add the following code to **Application Text > Formats > com.display.name.format**: `%MN`. For more information, see [“Modifying how the names of users are displayed” on page 450](#). The middle name is not stored in OpenPages.

6. Click **Validate**.

If a required field is missing or contains an incorrect value, a message is displayed.

7. After you successfully validate the information, click **Save**.

Provisioning users

Your ability to create a new user, modify user accounts, and copy access from one user to another is based on your administrative permissions and the way user provisioning is configured in your system. The user-provisioning options that you see in the product are determined by your permissions and configuration.

You can delegate administrative capabilities to specific administrators to give them the ability to perform certain user-provisioning functions. For example, you could delegate permission to two administrators to manage user passwords, and delegate permission to three other administrators to create users and update group memberships.

For information about which administrator permissions are required for each of the user-provisioning functions, see [Table 38 on page 43](#).

Creating user accounts

You create new user accounts on the **Create User** page.

Before you begin

Before you create a new user, see “[Planning user administration](#)” on page 40.

About this task

Depending on your permissions and user provisioning configuration, you can copy access from an existing user to a new one. You can also copy access from one existing user to another. For more information, see “[Modifying user accounts](#)” on page 49.

Depending on your delegated administrator permissions, you can perform certain functions when you create a user account, such as associating group memberships and assigning roles. For information about which permissions you need for each operation, see “[Administrator permissions for user-provisioning functions](#)” on page 43.

Procedure

1. Click  > **Users and Security** > **Users**.
2. Click **New User**.

Note: If you see a **Copy users from LDAP server** button, you can import user information from your organization's LDAP server. Click **Copy users from LDAP server** to search for and select a user. For information about configuring access to an LDAP server, see “[Configuring LDAP access for user provisioning](#)” on page 47.

3. Complete the information in **User Information** and **Password and Security**.

When you create user names and passwords, the following rules apply:

- User names are case-sensitive. For example, MyName and myname would be two unique users.
- User names can be up to 256 characters.
- User names can contain A-Z, a-z, 0-9, and any of the following special characters: @-!._:/_:*"\#%?<>

To exclude characters, including special characters, from user names, specify these characters in the **Illegal Characters** setting. For more information, see “[Exclude characters from user names](#)” on page 500.

- Passwords can contain up to 32 characters and cannot contain spaces.

If LDAP authentication is configured for your OpenPages application, you can specify how a user is authenticated when the user logs in to OpenPages. Click **Authenticate from**.

- If you want the user to authenticate by using OpenPages, select **Native**.
 - If you want the user to authenticate by using an LDAP server, select the LDAP server from the list. If you do not see any LDAP servers in the list, no LDAP servers are configured for user authentication.
4. In the **Locale and Profiles** section, you can change the user's locale, select a **Current profile**, and select **Allowed user profiles**. You can also see **Allowed group profiles** after you associate the user with one or more groups that have associated profiles.
 5. If you have the necessary permissions, you can copy access from another user to determine the starting point for a new user's attributes, such as group memberships, role assignments, and reports access.
- In **Copy Access From**, click **Select user to copy from**. Type a user name, first name, last name, or email address. Select a user, and then click **Copy**. When you click **Save**, the new user is updated with the access settings of the source user. Personal filters are not copied.
6. Click **Save**.
 7. In the **Group Memberships** section, perform the following actions to assign group memberships:

- To select group memberships, click **Associate Groups** and select the check boxes next to the groups to which you want the user to be a member.
 - To delete group memberships, click  next to the membership that you want to remove.
8. In the **Role Assignments** section, you can view the user's role assignments. To add role assignments, click **Assign Roles**.
9. In the **Reports Access** section, you can view the user's reports access.

Modifying user accounts

You can view and modify the details of an existing user account, such as all the user's group memberships, role assignments, and profiles.

Before you begin

Before you modify user information, see [“Planning user administration” on page 40](#).

About this task

Depending on how user provisioning was configured in your system, you might be able to copy access from one user to another. For information about copying access, see [“Copying access from one user to another” on page 50](#).

Depending on your delegated administrator permissions, you can perform certain functions when you modify a user account, such as editing user information, enabling or disabling a user account, and changing group memberships. For information about which permissions you need for each editing operation, see [“Administrator permissions for user-provisioning functions” on page 43](#).

There are some constraints on your ability to make changes. For example, you cannot disable or lock yourself, the default Super Administrator (OpenPagesAdministrator), or the OPSystem user. You cannot remove a user from special user groups that contain all users, or all users who are not associated with any other user group.

If you are logged in as a Super Administrator, you can add or remove super administrator status from other user accounts. For more information, see [“Creating a Super Administrator” on page 42](#).

Procedure

1. Click  > **Users and Security** > **Users**.
2. Search for the user account that you want to modify.
3. In the **User Information** section, you can perform one or more of the following actions:
 - Edit user details, such as email, first name, and last name. You cannot change a user name.
 - Disable and enable a user account. When an account is disabled, the user of that account is prevented from logging in, and the user is displayed as inactive and grayed out in user selector lists. If necessary, you can re-enable a disabled user account. User accounts cannot be deleted through the user interface in IBM OpenPages. Depending on how your system is configured, in addition to disabling the user, you can choose to remove their locale, profile, group membership, role assignment, or reports access.

Tip: If you want to prevent a user from logging in, but you still want the user to appear in user selectors, disable the user and then update the user selectors to set **Include Disabled** to **True**. For more information, see [“Defining user/group fields” on page 173](#).

- Lock and unlock a user account. Depending on your configuration, users might be locked automatically if they exceed a set number of unsuccessful login attempts. When an account is locked, the user of that account is prevented from logging in. The user is displayed as active but locked in user selector lists, and they can be selected. If you do not want the user to appear as active and selectable in user selector lists, disable the user account instead.

- Reset the user's password or force the user to change the password the next time they log on. Passwords can contain up to 32 characters and cannot contain spaces.

Important: If you use IBM OpenPages Loss Event Entry, do not modify the dedicated users' passwords by using OpenPages. Always use the Loss Event Entry Configuration tool. Also, the **User cannot change password** and **Password never expires** options must be selected for the dedicated user accounts.

If LDAP authentication is configured, you can also change the authentication method for the user. Click **Reset Password**, and then click the **Authenticate from** list.

4. In the **Locale and Profiles** section, you can change the user's locale, select a different **Current profile**, and change the **Allowed user profiles**. You can also see **Allowed group profiles**.
5. In the **Group Memberships** section, you can add and remove group membership assignments by clicking **Associate Groups**.
6. In the **Role Assignments** section, you can add role assignments by clicking **Assign Roles**.

You can remove role assignments that were assigned directly to the user. You cannot remove role assignments that are inherited from group memberships.

When you remove a role from a user or group, the role assignment is explicitly removed from the user or group on a given entity. The user is not, however, disassociated from the security domain.

7. In the **Reports Access** section, you can view the reports folder access that was assigned directly to the user and inherited from group memberships.

What to do next

If you removed a role assignment from a user or group, disassociate the user from the security domain.

Copying access from one user to another

You can copy a user's locale, profiles, group memberships, and direct role assignments. You can also copy direct reports access attributes to another user.

Before you begin

Before you copy access from one user to another, see [“Planning user administration” on page 40](#).

To copy access from one user to another, you must be granted **Manage** permission at the top-level group and **Assign Role** and **Manage** permissions at the root security domain. If you do not have these permissions, you cannot see the **Copy Access From** option.

Administrators with **Settings** application permission can use the user provisioning registry settings to establish the following copy access behavior:

- Determine whether the copy operation is allowed and which users, including inactive users, can be used as sources for the copy operation. For more information, see [“Users Can Copy Access From” on page 481](#) and [“Copy Access From Inactive” on page 480](#).
- Specify which attributes are copied by the copy operation. For more information, see [“Copy User Info Attributes” on page 480](#).
- Determine whether the copy operation adds to or replaces the user's existing attributes. For more information, see [“Copy User Info Choice” on page 480](#).

Procedure

1. Click  > **Users and Security** > **Users**.
2. Search for the user account that you want to modify.

Note: You can also copy access from an existing user when you are creating a new user. For more information, see [“Creating user accounts” on page 48](#).

3. From the left pane, click **Copy Access From**.
4. Search for the user that you want to use as the source.
5. Click **Copy**.

Note: Personal filters are not copied.

Creating an organizational group

Users with the correct permissions can create groups. Groups can contain other groups and users, and inherit application permissions from the groups that they belong to.

Procedure

1. Click  > **Users and Security** > **Domains & Groups**.
2. Click **Groups**.
3. Expand the list and click the name of the group to which the new group belongs. If no higher-level group for the new group exists, select the **Workflow, Reporting and Others** group.
4. From the selected group page, go to the **Groups** section and click **New**.
5. Complete the required information for the new group and click **Add**. The parent group's page is displayed with the new group listed in the **Groups** section.
6. Open the group from the **Groups** tab and complete the remaining sections:
 - **Administrators & Permissions**
 - **Groups**
 - **Users**
 - **Role Assignments**
 - **Permissions**

Associating and disassociating a group

You can associate and disassociate groups from other groups.

When you disassociate a group and that group does not belong to any other IBM OpenPages with Watson group, the group is listed under the special group **Workflow, Reporting and Others** > **Standalone Users and Groups**. You cannot add and remove groups directly from the **Standalone Users and Groups** group.

When you add an existing group to another group, the disassociated group is still available in the group selector list.

Procedure

1. Click  > **Users and Security** > **Domains & Groups**.
2. Click the **Groups** tab.
3. Expand the list and click the name of the group to which you want to associate another group, or to which the soon-to-be-disassociated group belongs.
4. Go to the **Groups** section.
5. Click **New** to create a group and associate it to the selected group. For more information, see [“Creating an organizational group” on page 51](#).
6. Click **Add** to add an existing group to the selected group.
7. Click **Remove** to remove a group.

Defining application permissions

You can define access permissions for IBM OpenPages with Watson.

The following methods of defining permissions are available:

- In **Role Templates** - this is the preferred method for granting users or groups application permissions.

Note:

- Both application permissions and ACLs are included in the role definition process. When a role is assigned to a user or a group on any business entity or security context point, that user or group automatically acquires the application permissions defined in that role template.
- When a user or group is assigned multiple roles, the user or group accumulates the application permissions that are defined in the various roles. Application permissions are granted by the role (not the security context point) and apply in all situations where the user has the correct ACL access. For example, users with Read permission to Business Entities and the **Audit Trail** application permission are able to view the **Activity** tab for those Business Entities.

For more information, see “[Role templates](#)” on page 75.

- As part of an organizational group definition - this method is provided for backward compatibility for upgrade customers and for administering system-wide organizational groups. Organizational groups can be created under the **Workflow, Reporting and Others** root folder on the **Users, Groups and Domains** page. For more information, see “[Creating an organizational group](#)” on page 51.

Setting group application permissions

By setting application permissions on a group (either through a role template or on organizational groups), you can control, for example, whether users in that group can lock objects, view audit trail information, and create reporting periods.

To delegate group security management permissions to administrators, see “[Delegate administrator permissions](#)” on page 42.

To assign application permissions for a role, see “[Accessing Role Templates](#)” on page 75.

Procedure

1. Click  > **Users and Security** > **Domains & Groups**.
2. Click **Groups**.
3. Expand the list and click the name of the group whose application permissions you want to view or modify.
4. On the selected group, go to the **Permissions** section.

Tip: Most of the application permissions in IBM OpenPages with Watson are grouped under the SOX heading. Selecting the SOX permission selects all the permissions under that heading. This is only advisable for administrative level users.

For a description of the various permissions, see “[Types of application permissions](#)” on page 52 and “[Application permissions not contained under the SOX heading](#)” on page 58.

5. To modify application permissions for a group, click **Edit**, make the required changes, and then click **Done**.
6. To assign user and group management permissions to selected users, see “[Delegate administrator permissions](#)” on page 42.

Types of application permissions

Administrators can use a set of application permissions to limit the activities of the various users and user groups that can access the IBM OpenPages with Watson application. The application permissions reside under the SOX permissions heading and can be applied to OpenPages with Watson user groups.

Important: If the changes to application permissions result in changes to menus, the menu changes do not appear until users log out and then log back in to the application.

Users are generally granted applicable permissions by being assigned to role templates that include those permissions.

Administration permissions

When you create an administrative-level group, you must grant them Administration permissions.

Table 39. Administration application permissions	
Permission	Description
Application Text	Allows users and members of user groups to view and edit locale-specific application label values. For more information, see “ Localizing application text ” on page 447.
Ascent Feed	Allows users and members of user groups to configure the import of Ascent Reg Tech data by using the Ascent job in the Scheduler.
Bulk Update All Fields	Allows users to use the Bulk Update feature on all fields in grid views. For more information, see “ Designing a Grid View ” on page 256.
Calculation	Allows users and members of user groups to create, delete, and modify calculation definitions by using  > Solution Configuration > Calculations . For more information, see Chapter 15, “Configuring GRC Calculations,” on page 327 .
Currencies	Allows users and members of user groups to administer currencies. For more information, see “ Modifying currency exchange rates ” on page 167.
Dashboards	Allows administrators to create and manage dashboards by using  > Solution Configuration > Dashboards . For more information, see “ Home page, dashboard, and tabs ” on page 230
Encryption Keystore	Allows administrators to configure the encryption keystore by using  > Users and Security > Encryption Keystore . For more information, see “ Encryption ” on page 104.
ExportConfiguration	Allows users to access the environment migration tool to export configuration items for import into another system. Read and write access to the Migration Documents folder is also required. For more information, see Chapter 26, “Migrating OpenPages environments,” on page 719 .
FastMap	Allows a user to import object data and to view imports performed by other users. Import allows users to import object data and to see their import history using the FastMap Import menu item. View all history allows users to view imports performed by other users. When a user has this permission, the Created By column is added to the grid on the FastMap Import tab. For more information, see Chapter 28, “Using FastMap,” on page 767 .

Table 39. Administration application permissions (continued)

Permission	Description
Field Groups	Allows users and members of user groups to view and manage the configuration of field groups through the  > Solution Configuration > Object Types menu item and the Field Groups section.
ImportConfiguration	Allows users to access the environment migration tool to import configuration items that are exported from another system. Read and write access to the Migration Documents folder is also required. For more information, see Chapter 26, “Migrating OpenPages environments,” on page 719 .
LDAP Server	Allows Super Administrators to configure the LDAP server for user provisioning. For more information, see “LDAP and user provisioning” on page 46 .
Logs	Allows users to view and manage the application server log files by using the  > Other > Logs menu item. Read and write access to the LogCollector Documents folder is also required.
Notification Manager	Allows Super Administrators and users to run the Notification Manager tool. For more information, see Appendix A, “The Notification Manager,” on page 925 .
NPS	Allows users and members of user groups to configure the Net Promoter Score (NPS) with the  > Integrations > NPS Settings menu item.
Object Profiles	Allows users and members of user groups to view and manage profiles, which include object types, through the  > Solution Configuration > Profiles menu item.
Object Reset	Allows users and members of user groups to reset objects for a new reporting period. For information on governing reset behavior, see Chapter 19, “Reporting periods, object resets, and rulesets,” on page 457 .
Object Text	Allows users and members of user groups to view and edit locale-specific object label values. For more information, see “Localizing object text” on page 445
Object Types	Allows users and members of user groups to view and manage object types through the  > Solution Configuration > Object Types menu item. Allows users and members of user groups to view and manage solution schema visualizations, through the  > Solution Configuration > Solutions menu item.
RapidRatings Feed	Allows users and members of user groups to configure and run the RapidRatings job in the Scheduler. The job imports data from RapidRatings.
RegTrack Feed	Allows users and members of user groups to configure the import of Reg-Track data through the  icon on the Regulatory Compliance > Reg-Track Regulatory Events page.

Table 39. Administration application permissions (continued)

Permission	Description
Reporting Framework	Allows users and members of user groups to generate and manage the reporting framework. For more information, see “ Generating the reporting framework ” on page 814.
Reporting Framework Configuration	Allows users and members of user groups to administer and configure the reporting framework. See Chapter 29, “Configuring and generating the reporting framework,” on page 799.
Reporting Periods	Allows users and members of user groups to work with reporting periods through the  > System Configuration > Reporting Periods menu item. For more information, see Chapter 19, “Reporting periods, object resets, and rulesets,” on page 457.
Reporting Schema	Allows users and members of user groups to manage the Reporting Schema. See Chapter 7, “Managing the reporting schema ,” on page 117.
RiskLens Feed	Allows users and members of user groups to configure and run the RiskLens job in the Scheduler. The job imports data from RiskLens.
RiskRecon Feed	Allows users and members of user groups to configure and run the RiskRecon job in the Scheduler. The job imports data from RiskRecon.
Role Templates	Allows users and members of user groups to view, add, and manage roles through the  > Users and Security > Role Templates menu item. .
Rules Engine	Allows users and members of user groups to view, create, and manage rules through the  > Solution Configuration > Regulatory Event Rules menu item. If you are using the Thomson Reuters connector, users access the Rules Engine through the TRRI Rules Engine link on the Regulatory Compliance > TRRI Regulatory Events page. If you are using the Wolters Kluwer connector, users access the Rules Engine through the Wolters Kluwer Rules Engine link on the Regulatory Compliance > WK Regulatory Events page.
Scheduler	Allows users and members of user groups to create and manage scheduled jobs through the  > Solution Configuration > Scheduler menu item.
Search	Allows users and members of user groups to manage and maintain global search operations through the  > System Configuration > Global Search menu item. For more information, see Chapter 21, “Configuring the global search feature,” on page 517.
Security Rules	Allows users and members of user groups to manage and maintain security rules. For more information, see “Security rules” on page 80.

Table 39. Administration application permissions (continued)

Permission	Description
Security Scorecard Feed	Allows users and members of user groups to configure and run the SecurityScorecard job in the Scheduler. The job imports data from SecurityScorecard.
Settings	Allows users and members of user groups to view and manage settings. For more information, see Chapter 20, “Viewing the Configuration and Settings page,” on page 473 .
Solutions	<p>Allows users and members of user groups to use the  > Solution Configuration > Solutions menu item. .</p> <p>Allows users and members of user groups to use the  > Solution Configuration > Themes menu item.</p>
SupplyWisdom Feed	Allows users and members of user groups to configure and run the import of Supply Wisdom data by using the SupplyWisdom job in the Scheduler.
Tagging	<p>Allows users and members of user groups to enable and disable the Tagging feature, and create, edit, and disable tags.</p> <p>This permission controls whether the  > Solution Configuration > Tags menu item is displayed.</p>
Task Focused UI	<p>Allows users and members of user groups to create and manage views in the View Designer. For more information, see “Using the View Designer” on page 272.</p> <p>This permission also controls whether the  > Other > Display Debug Info menu item is displayed.</p>
TRRI Feed	Allows users and members of user groups to configure the import of Thomson Reuters Regulatory Intelligence (TRRI) data through the  icon on the Regulatory Compliance > TRRI Regulatory Events page.
Watson Assistant	Allows users and members of user groups to use the  > Integrations > Watson Assistant menu item.
Watson Language Translator	Allows users and members of user groups to use the  > Integrations > Watson Language Translator menu item.
Custom Machine Learning Models	Allows users and members of user groups to use the  > Integrations > Custom Machine Learning Models menu item.
Watson Mapping and Taxonomy Suggestions	Allows users and members of user groups to use the  > Integrations > Mapping and Taxonomy Suggestions menu item.
WK Feed	Allows users and members of user groups to configure the import of Wolters Kluwer data through the  icon on the Regulatory Compliance > WK Regulatory Events page.

Table 39. Administration application permissions (continued)

Permission	Description
Workflow	Allows users and members of user groups to create workflow definitions and terminate workflow instances through the  > Solution Configuration > Workflows menu item. For more information, see Chapter 16, “Configuring GRC Workflow,” on page 369 .

IBM CommandCenter Studio permissions

This application permission allows users and members of user groups to access IBM Cognos Analytics from IBM OpenPages with Watson.

Table 40. IBM Command Center Studio permission

Permission	Description
Cognos Analytics	This application permission enables access to IBM Cognos Analytics through the Analytics link in the primary menu. Use IBM Cognos Analytics to access your Cognos software and corporate data. Depending on your access permissions, you can create, update, run, and distribute reports, dashboards, stories, and cubes, create and run agents, or schedule entries.

Audit Trail permission

The **Audit Trail** application permission allows users and members of user groups to view historical information about object for the selected Reporting Period.

Users can access the **Activity** tab in Task Views.

For more information, see [“Reporting period interactions” on page 457](#) and the *IBM OpenPages with Watson User Guide*.

Note:

- When you copy objects, change histories are not copied with the object. The copy of the object has no change history because it is a new object.
- When you add new fields to an object type, the OpenPages with Watson administrator might see a blank to blank change in the change history because the fields were not previously available.

Issues permission

This application permission allows users and members of user groups to view the list of Issues through the **Issues** menu item on the **Remediation** menu.

Note: This application permission is in effect only for customers who upgraded or migrated and who have not yet migrated their access controls to the role-based security model. For new, first-time installations, this permission is not honored.

Watson permissions

- Watson Assistant UI:** Users with this permission have access to the user interface that enables them to interact with IBM Watson Assistant in OpenPages.

- **Watson Language Translator UI:** Users with this permission can use IBM Watson Language Translator

to view translated text in Task Views by using the  icon. It also allows access to the  icon from administrator tasks.

View Admin tab

Users with the **View Admin tab** permission can see Admin views on the Admin tab of an object instance page.

View Locks permission

Users with the **View Locks** permission can view the existing locks on objects. The **View Locks** permission does not grant the right to lock or unlock an object - for that you need either the **Lock** permission or the **Unlock** permission.

Application permissions not contained under the SOX heading

Some application permissions are not contained under the SOX permission heading, but still have an impact on OpenPages with Watson application behavior. Application permissions determine what functional areas and administrative operations a user or group is able to perform. Typically, users do not require these application permissions.

Users are generally granted the applicable permissions by being assigned to role templates that include those permissions.

All permission

Grants users and members of user groups all permissions and access to every functional and administrative area within OpenPages with Watson (web and server).

Administration permissions

The Administration permissions grant users and members of user groups the ability to archive and restore document versions and to enable and disable System Admin Mode.

<i>Table 41. Administration permissions</i>	
Permission	Description
Archive Management	Allows group members to archive and restore document versions.
Enhanced Error Messaging	Allows group members to view error messages in detail.
System Administration Mode	Allows group members to enable and disable System Admin Mode and perform certain administrative functions. For details see, " Enabling and disabling System Admin Mode " on page 37.

API permissions

This permission enables users to run tools and utilities that use the REST API.

Table 42. API permissions

Permission	Description
Administration > Background Process > Get Process Info	<p>Used for the following items:</p> <ul style="list-style-type: none"> Required to run ObjectManager operations. <p>To run load, validate, and batch operations with ObjectManager, users also need the SOX > Administration > ImportConfiguration permission.</p> <p>To run dump operations with ObjectManager, users also need the SOX > Administration > ExportConfiguration permission.</p> <ul style="list-style-type: none"> Controls whether the  > Other > Background Processes menu item is displayed.
Administration > Background Process > Terminate Process	<p>Required to run the following API processes:</p> <ul style="list-style-type: none"> In the OpenPages API: <code>ProcessService.terminateProcess</code> In the OpenPages GRC REST API: <pre>grc/api/processes/{processid}?action=terminate</pre>

Files permissions

This application permission grants all administrative permissions under the Files grouping that are related to managing files and folders.

Table 43. Files permissions

Permission	Description
Add Folders	Allows group members to create and add new folders.
Cancel Checkout	Allows group members to cancel the file check-out process for associated files that were checked out by others. When a file check-out is canceled, the file is checked back into the system without applying any changes and no new version of the file is created. Restriction: This permission applies only to file attachments (of the SOXDocument object type).
Lock	Allows group members to lock objects, regardless of sign-off or ACL restrictions.
Reassign Primary Association	Allows members of the user group to reassign primary parent associations and view the Make this object Primary icon on the Parent tab of an object, where <i>object</i> is the object type.
Remove All Tree Locks	Allows members of the user group to unlock resources and/or resource subtrees.
Unlock	Allows group members to unlock objects.

Publishing permissions

Super administrators and members of the OPAdministrators group can add folders, pages, and templates without any specific permissions.

Only super administrators and members of the OPAdministrators group can copy, move, and delete folders, pages, and templates.

Users can add folders, templates, and pages if they have the corresponding permission and if they have Write permission to the folder.

Table 44. Publishing permissions	
Permission	Description
Add Folders	Allows users to add report folders by using New Folder on the Pages and Templates page.
Add Pages	Allows users to add reports by using the Add Cognos Report button on the Pages and Templates page. Allows users to add report pages by using New Page on the Pages and Templates page.
Add Templates	Allows users to add report page templates by using New Page Template on the Pages and Templates page.

Configure password requirements

IBM OpenPages with Watson supports the use of strong passwords (passwords that include letters, numbers, and symbols).

It also allows administrators to enforce mandatory password changes and other password behavior.

Note: Configuring password behavior in OpenPages with Watson does not apply if you use single sign-on (SSO), such as LDAP or Microsoft Active Directory. Your internal IT policies dictate password behavior within the product.

Configuring password policies

The IBM OpenPages with Watson allows administrators to modify the password policies for the application.

Using the password policies, administrators can enable strong passwords and control whether user passwords must be changed after a certain length of time.

To access the password settings, go to  > **System Configuration** > **Settings** > **Platform** > **Security** > **Password**

Table 45. Password Settings	
Setting	Description
Encryption Administrator	The user name who is allowed to change the password encryption algorithm and the encryption key.
Strong Policies - Character Groups 1-4	These settings allow the administrator to configure the strong password policies for the application. Each Character Group takes a comma-separated list of characters. By default, these groups are empty. If strong passwords are enabled, each password is required to contain at least one character from each group. If a group is empty, that group is ignored. Important: You cannot include the comma as a required character in a strong password.

Table 45. Password Settings (continued)

Setting	Description
Strong Policies - Enabled	If the value is set to: <ul style="list-style-type: none">• true - then users are required to enter strong passwords when they specify their user password.• false - then users are not required to enter strong passwords when they specify their user password. This value is set by default.
Enabled	Sets whether the password policies are active or not. The default value for this setting is false.
Maximum Length	Sets the maximum length of the password. The default value for this setting is 32.
Minimum Length	Sets the minimum length of the password. The default value for this setting is 6.
Notify Before Days	Sets the number of days before a user's password expires that the user is shown a warning message at logon about their password expiring.

Updating the password encryption algorithm

To update the password encryption algorithm, you use the Update Password Encryption Algorithm (UPEA) tool.

Note: The topics in this section are not applicable in IBM OpenPages for IBM Cloud Pak for Data.

Before you use the UPEA tool, ensure that you complete the following tasks:

- [“Verifying the current encryption algorithm” on page 61](#)
- [“Verifying the environment” on page 62](#)
- [“Configuring the security provider in the java.security file” on page 62](#)
- [“Preparing passwords in the aurora.properties file and the op-backup-restore.env file for reencryption” on page 63](#)
- [“Updating the Users table to change passwords” on page 63](#)

You run the tool from the command line as follows:

<OP_HOME>\bin\UpdatePasswordEncryptionAlgorithm.cmd (Windows)

<OP_HOME>/bin/UpdatePasswordEncryptionAlgorithm.sh (Linux)

Tip: You can also run the tool from a remote system, such as your laptop. For more information, see [“Installing tools and utilities \(IBM OpenPages with Watson\)” on page 692](#)

You can use the UPEA tool to do the following tasks:

- Change the encryption algorithm from 3DES to AES.
- Change the AES encryption key - this is the default encryption algorithm.

Verifying the current encryption algorithm

If you have a legacy system, verify the name of the current encryption algorithm before you run the UPEA tool to change the algorithm to AES as follows.

Procedure

1. Log on to a machine with SQL*Plus and access to the database server.
2. Execute the following SQL statement:

```
select algorithmname from encryptionmodules where inactive=0;
```

3. When you are finished, log out of SQL*Plus.

Results

If the SQL statement returns the name:

- 3DES, then run the UPEA tool to change the encryption algorithm to AES.
- AES, then you already have the AES encryption algorithm. If you want, you can use the UPEA tool to change the AES encryption key.

Verifying the environment

The following tasks must be completed before you run the UPEA tool.

- An IBM OpenPages with Watson system must be properly installed and functioning on the machine.
- A full backup of the OpenPages with Watson database must be completed. For more information, see [Chapter 22, “Using IBM OpenPages with Watson utilities with Db2 databases,” on page 545](#) or [Chapter 23, “Using IBM OpenPages with Watson utilities with Oracle databases,” on page 577](#).
- Ensure that all OpenPages with Watson servers are started and that no users are logged on to the system during the password encryption update.

Note: For details on starting and stopping servers in Windows and Linux environments, see [“Starting application servers” on page 709](#).

Configuring the security provider in the java.security file

The security provider must be specified in the `java.security` file.

About this task

Note the following recent name changes:

- `bcprov-jdk14-145.jar` is `bcprov-jdk15to18-1.68.jar` in 8.2.0.2 or later
- `org.bouncycastle145.jce.provider.BouncyCastleProvider` is `org.bouncycastle.jce.provider.BouncyCastleProvider` in 8.2.0.2 or later
- `CAMCryptoBC` is `BC` in 8.2.0.2 or later

Procedure

Verify that the `BouncyCastleProvider` security provider has been added to the `java.security` file as follows:

a) Open a command or shell window on the application server.

b) Go to:

```
<JAVA_HOME>/jre/lib/security
```

Where:

`<JAVA_HOME>` is the installation location of IBM SDK, Java Technology Edition. For example:

- On Windows: `C:\IBM\java_8.0_64`
- On Linux: `/opt/IBM/java_8.0_64`

c) Make a backup copy of the `java.security` file before you modify it.

d) Open the `java.security` file in a text editor of your choice.

e) Locate the following property in the file:

```
security.provider.<#>=
```

f) If the `BouncyCastleProvider` security provider is not present, add the following line:

```
security.provider.<#=org.bouncycastle.jce.provider.BouncyCastleProvider
```

Where: The number sign, <#>, is one increment above the last number in the list. For example, security.provider.9.

- g) Save and close the file.

Preparing passwords in the aurora.properties file and the op-backup-restore.env file for reencryption

You can reencrypt the passwords that are in the aurora.properties and op-backup-restore.env files. By default, the files are in the <OP_Home> directory.

For Microsoft Windows operating systems, the default installation directory of OpenPages with Watson is C:\IBM\OpenPages.

For Linux operating systems, the default installation directory of OpenPages with Watson is /opt/opuser/IBM/OpenPages.

Procedure

1. Open a command or shell window on the application server.
2. Go to the <OP_Home>|aurora|conf directory.
3. Edit the aurora.properties file in the conf directory.
 - a) Make a backup copy of the file.
 - b) Open the file in a text editor of your choice.
 - c) Search the file for properties that include the string password.
 - d) Change all password values after the equal sign to plain text.
 - e) Save and close the file.

Note: The passwords are encrypted when you restart the servers.

4. Edit the op-backup-restore.env file in the <OP_Home>|aurora|bin directory.
 - a) Make a backup copy of the file.
 - b) Open the file in a text editor of your choice.
 - c) Search the file for properties that include the string PWD.
 - d) Change each password value to plain text.
 - e) Save and close the file.

Note: The passwords are encrypted when you restart the servers.

Updating the Users table to change passwords

Updating the Users table to change passwords with the UPEA tool applies only to upgraded databases.

Procedure

1. On a computer that has access to the database server, connect to the OpenPages database as the OpenPages database user.
2. Run the following SQL statement to update the Users table so that passwords can be changed:

```
update users set flag_can_change_password=1 where actorid not in (select actorid from actorinfo where name = 'OPSystem');
```

UPEA tool syntax and parameters

The UPEA tool defines the parameters of the password encryption algorithm.

UPEA syntax

The syntax of the UPEA tool is detailed in the following section:

```
UpdatePasswordEncryptionAlgorithm
  -Mode [CA|CK]
  -AlgorithmName [AES]
  -ProviderName BC
  -ProviderClass org.bouncycastle.jce.provider.BouncyCastleProvider
  -Username <OpenPagesAdministrator>
  -Password <OpenPagesAdministrator password>
  [-KeySize 128]
  [-?]
```

Note the following recent name changes:

- bcprov-jdk14-145.jar is bcprov-jdk15to18-1.68.jar in 8.2.0.2 or later
- org.bouncycastle145.jce.provider.BouncyCastleProvider is org.bouncycastle.jce.provider.BouncyCastleProvider in 8.2.0.2 or later
- CAMCryptoBC is BC in 8.2.0.2 or later

The following table describes the parameters of the UPEA tool.

Table 46. UPEA parameters	
Parameter	Description
-Mode	Required. Use to specify the mode in which the tool should run. Possible modes are: <ul style="list-style-type: none">• CA (for Change Algorithm) — used to switch the encryption algorithm from 3DES to AES.• CK (for Change Key) — used to change the AES encryption key.
-AlgorithmName	Required. Use to specify the type of encryption algorithm to use. The only valid value is AES.
-ProviderName	Required. Use when you change algorithms to the AES encryption algorithm only. Has only one valid value: BC.
-ProviderClass	Required. Use only in conjunction with -ProviderName to specify the class for the new encryption algorithm. Has only one valid value: org.bouncycastle.jce.provider.BouncyCastleProvider
-Username	Required. Use to specify the user name to use when you modify the user passwords. Must be the same as the user specified in the OpenPages Platform Security Password Encryption Encryption Administrator setting.
-Password	Required. Use to specify the password to the Encryption Administrator account.
-KeySize	Optional. Use to specify the length of the AES encryption key. The only valid value is 128. If an invalid value is given, or no value is provided, the default value of 128 is used.
-?	Optional. Displays the on-screen help for the UPEA tool.

Changing the password encryption algorithm to AES

You can run the UPEA tool to change the password encryption algorithm from 3DES or OP-CUSTOM to AES, which is more secure. To do this task, you must be an Encryption Administrator.

Procedure

1. Edit the <OP_HOME>/aurora/conf/aurora.properties file and the <OP_HOME>/aurora/bin/op-backup-restore.env file and change any encrypted passwords to plain text.

- If you are using 3DES, look for lines that contain {3DES}.

For example, suppose the aurora.properties file contains the following line:
database.PASSWORD={3DES}Rj+steg+3eU7kb80+\=\=. The database password is encrypted with the 3DES algorithm. Replace the encrypted password with the password in plain text, for example, database.PASSWORD=db_password.

- If you are using OP-CUSTOM, the lines do not have an algorithm indicator. Look for encrypted passwords and change each of them to the password in plain text.

The passwords are encrypted with the AES algorithm when you restart the OpenPages with Watson services in step 3.

2. Open a command or shell window on the OpenPages application server.

Go to the <OP_HOME>/bin directory.

From the command or shell window, run the following command on a single line:

```
UpdatePasswordEncryptionAlgorithm.sh|.cmd -Mode CA -AlgorithmName AES  
-ProviderName BC  
-ProviderClass org.bouncycastle.jce.provider.BouncyCastleProvider -KeySize 128  
-Username <OpenPagesAdministrator> -Password <OpenPagesAdministratorPassword>
```

3. Restart all OpenPages services.

4. If you are using OpenPages to authenticate users, notify all users that their passwords have been reset to 0p3nP4g3s and that they must change their passwords the next time they log on to the system.

Note: If you are using Single Sign-On (SSO), LDAP, or another external system to authenticate users, passwords are not reset.

Changing the AES encryption key

At certain times, you might want to change the encryption key that is used by the AES encryption algorithm. You can change the encryption key by using the UPEA tool. To do this task, you must be an Encryption Administrator.

Procedure

1. Log on to the IBM OpenPages with Watson server as a user with administrative privileges.
2. Open a command or shell window and change directory to the <OP_Home>/bin directory.
3. From the command or shell window, run the following command on a single line:

Windows

```
UpdatePasswordEncryptionAlgorithm -Mode CK -AlgorithmName AES  
-Username <OpenPagesAdministrator> -Password <password>
```

Linux

```
./UpdatePasswordEncryptionAlgorithm.sh -Mode CK -AlgorithmName AES  
-Username <OpenPagesAdministrator> -Password <password>
```

Where: <password> is the password for the OpenPagesAdministrator account.

4. Restart OpenPages with Watson services for the changes to take effect.

Chapter 6. Security

Most of your security requirements can be handled in IBM OpenPages with Watson with folder-based security using role-based security. If you need to refine folder-based security, use security rules.

Role-based security

Use role-based security to define application permissions for each role and to set access control (Read, Write, Delete, Associate) for each object that is included in that role. All users in each role inherit the same security access controls.

Security rules

You can define two types of security rule:

- Record level security rules

Use record level security rules to control access to individual objects in a folder. For example, two GRC domains share a common organizational hierarchy. They share some common object instances, such as processes, but they do not want to share other object instances, such as risks and controls. If you do not create security rules on objects, folder-based security applies.

Record level security rules have the following access controls: Create, Read, Update, Delete, and Associate. The Write access control in folder-based security is split into Create and Update for security rules, which gives you more control over what users can and cannot do.

- Field level security rules

Use field level security rules to control access to individual fields within an object.

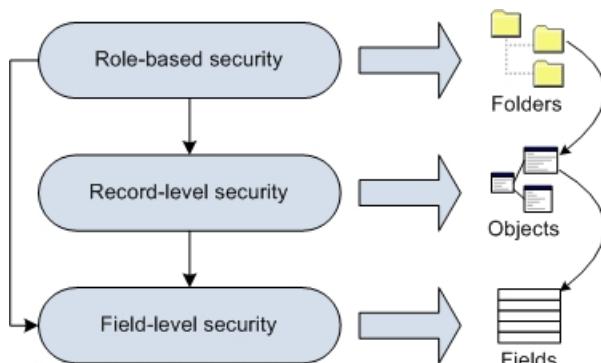


Figure 2. Levels of security

Role-based security and security rules differ from profiles and field dependencies because security is applied everywhere rather than in the OpenPages with Watson application only.

Role-based security model

A role-based security model provides a way for administrators to control user and group access to objects that are under a defined security point within the object hierarchy according to the role the user or group is expected to perform within the organization.

Typical security points are business entities, processes, or sub-processes (can also be set at lower security point levels if wanted).

Figure 3 on page 68 shows how various users and groups can have different permissions set for accessing business entities (a defined security point in the object hierarchy) and objects that are under a specific hierarchy.

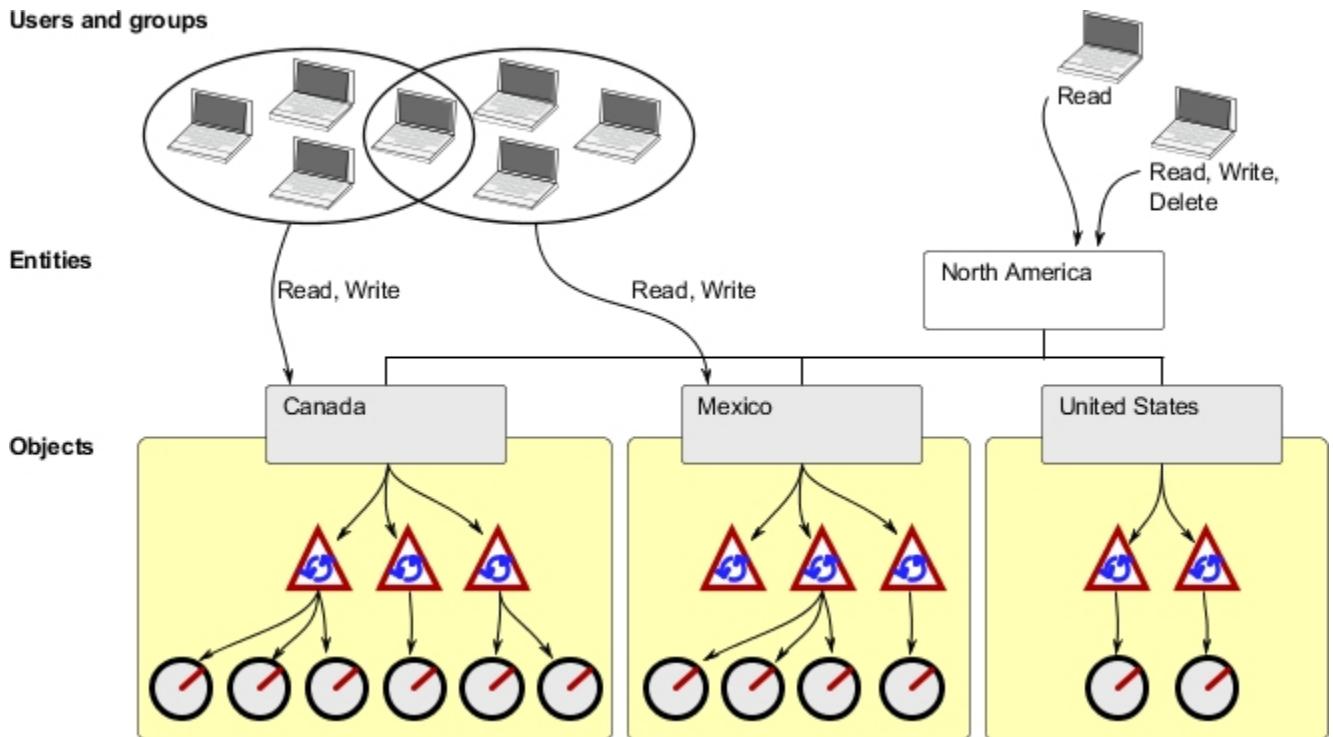


Figure 3. Security concepts in a hierarchy

Based on the type of security context points defined in your security model, such as Business Entity, Process, Control Objective or Risk Assessment, you can use a role template to define a set of permissions for a set of object types.

For each role template that you define, you can set the following:

- Access control (Read, Write, Delete, Associate) for each object type included in that role. For details, see [“Role-based access control permissions” on page 73](#).
- Application permissions for the role. For information about the various application permissions, see [“Defining application permissions” on page 51](#).

Important: These application permissions do not include administrative group and user security management permissions, such as resetting passwords, assigning roles, adding users, and so forth. To learn more about assigning group and user security management permissions to administrators, see [“Delegate administrator permissions” on page 42](#).

By assigning a role (an instance of a role template) to a user or group at specific security context point in the object hierarchy, you can control access to objects. Roles represent the usual or expected function that a user or group plays within an organization. Some examples of roles are: Finance Reviewer, Tester, External Auditor, System Administrator, Control Owner, Risk Assessor.

When you assign a role to a group or user, the security settings of that role template are acquired by that group or user and permissions are automatically granted, per the role template definition, to all objects below the specified security point.

For example, if a role were assigned to a user for a business unit (security context point), access control for specific object types under that security point would be set in the object hierarchy. Object types that were excluded from the role would be hidden from view, object types that were included would be visible and could be accessed by users and groups assigned to that role.

So that you can have a clear and accurate understanding of which users and groups have access to what and with which permissions, and what access control modifications were made in the system, you can run a variety of reports to view this data. For details on the types of configuration audit and security reports available to you, see the section [“Audit Reports folder” on page 126](#).

Security context points

The structure of the object hierarchy that is defined in your system also acts as the security context point to which access control can be assigned.

Roles (defined by role templates) are granted to specific security points in the object hierarchy, and permissions for a particular role are automatically granted to all objects that are created in the same location beneath that security point. If a role is assigned to a group on a top-level Business Entity, then all users of that group would have access to that business entity and would be able to access all objects under that entity as per the permissions in the role.

By default, the installation process automatically sets Business Entity (SOXBusEntity) as the security context point within the object hierarchy at which roles can be assigned.

Example

You have a regional office called North America and a sub-regional office called United States. When you create the business entity, the folder structure /BusinessEntity/North America/United States would automatically be created.

You also created a role template called Entity Owners that has access defined for the following object types:

- Business Entity
- Process
- Sub-process
- Control Objective
- Risk
- Control

When you assign the Entity Owners role template to the United States business entity, the following structure is automatically generated under the root folder of each object type:

```
/Processes/North America/United States  
/Sub-processes/North America/United States  
/ControlObjectives/North America/United States  
/Risks/North America/United States  
/Controls/North America/United States
```

Note: The folder structure /BusinessEntity/North America/United States does not need to be generated because it already exists (it was automatically created when the business entity was initially created).

Figure 4 on page 70 shows how access permissions (R=Read, W=Write, D=Delete, A=Associate) can be granted to specific objects in the hierarchy under the United States business entity security context point.

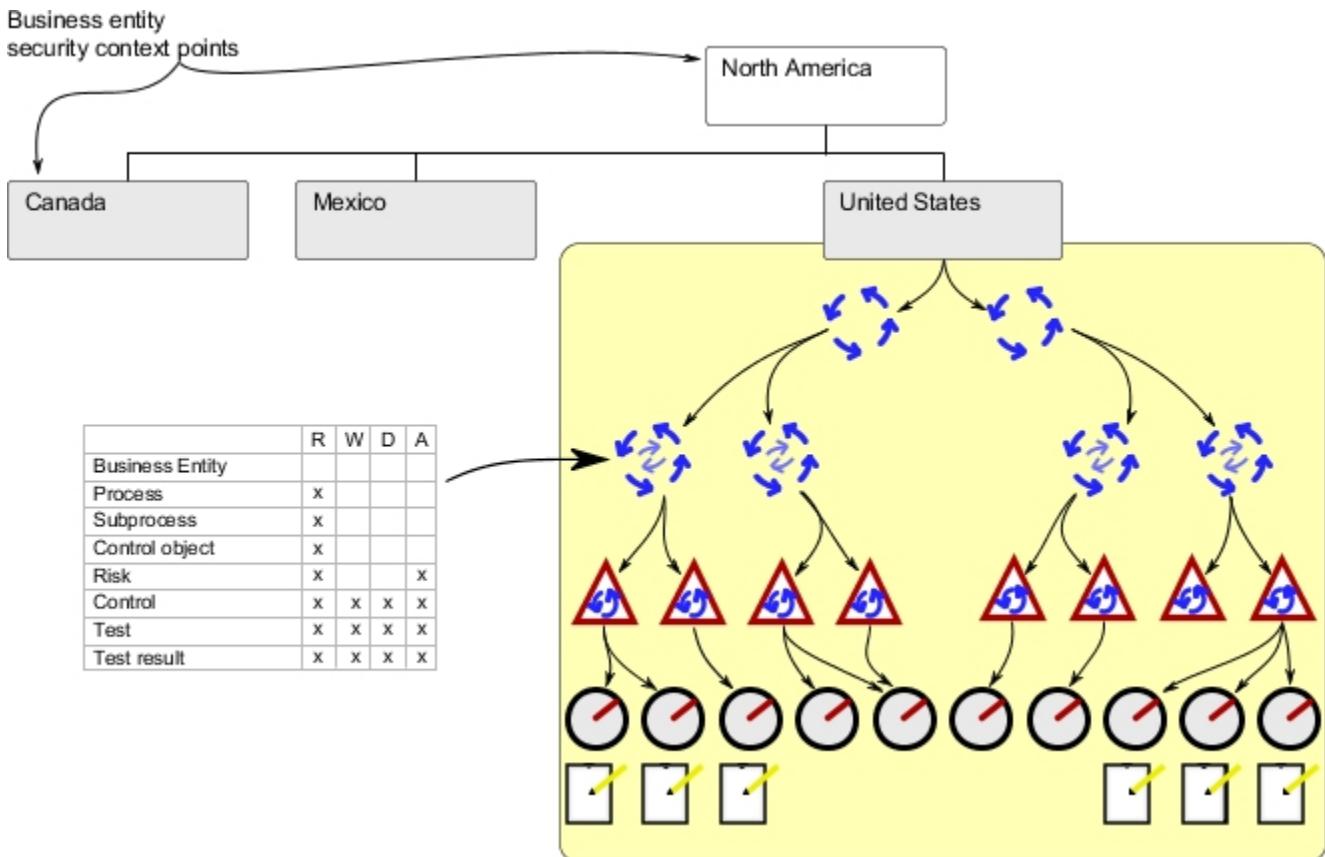


Figure 4. Business entity security context points

For details on assigning security management permissions to security domain group administrators, see “[Delegate administrator permissions](#)” on page 42.

Extending security context points

To achieve a finer level of control, it is possible to extend the security context point to other objects in the hierarchy (such as Business Entity-Process or Business Entity-Risk Assessment).

To achieve more control, change the Model setting. For more information, see “[Set the system security model](#)” on page 500).

Note: The Model setting is a system-wide setting. Switching the security model after data is loaded (or migrated) into the system is not recommended and requires assistance from IBM OpenPages with Watson Services.

To determine the optimal security context points for your organization, you need to evaluate your requirements for securing resources at lower security context points in your hierarchy. Extending the security context points to achieve a finer level of control does not prevent you from defining security at higher security context points.

Example

You extended the security context points to include Business Entity-Process. In this scenario, administrators could assign, for example, a “Process Role Template” to one or more users or groups on one or more Processes.

Permissions (Read, Write, Delete, Associate) in the “Process Role Template” could then be assigned to that Process security context point. The permissions in that template are applied to every object created beneath that point in the object hierarchy and to any object that is created in the future below that point.

Although users and groups who are assigned the "Process Role Template" would be able to navigate to and access Processes and child objects beneath a Process hierarchy, the details of the parent Business Entity would be hidden from them.

Note: Users who have roles that are assigned to a context security point within the Business Entity level only have only navigation access to the parent Business Entity. If users require the ability to view or modify the details of a parent Business Entity, then you must use an entity-based role template to grant explicit Read and/or Write permission to users at an entity security point.

The user interface in OpenPages with Watson does not allow breaking folder ACL inheritance on any folder on which role-based access control is assigned. Administrators are strongly advised not to break folder inheritance using ObjectManager or any other application interfaces on any object type folders as this will cause role-based security to fail.

[Figure 5 on page 71](#) shows how access permissions can be granted when the security context points are extended to include Process objects as security points to achieve a higher level of control.

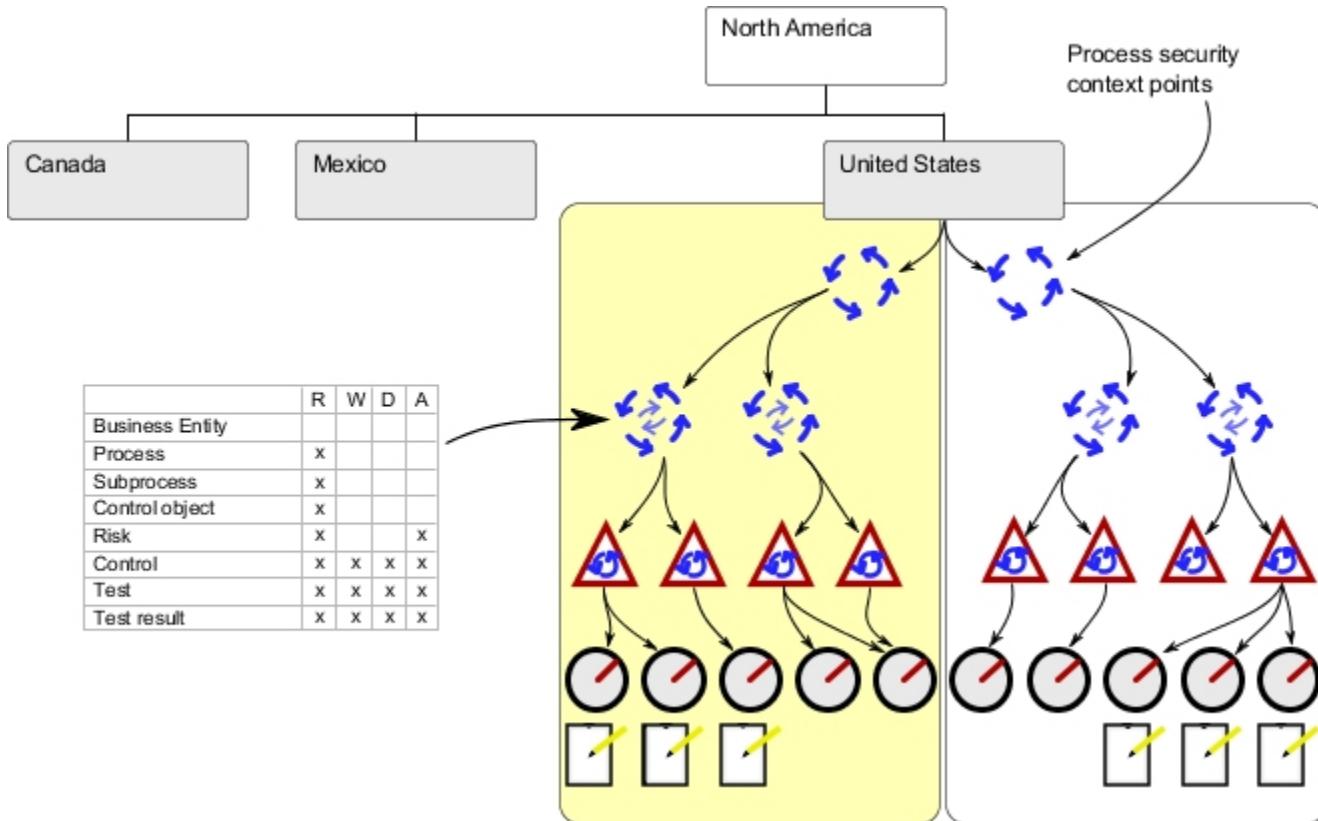


Figure 5. Business entity and process extended context points

Reporting framework and multiple security context points

In a security model that contains multiple security context points, objects that form a "triangle" relationship have implications for the reporting framework.

Triangle relationships are formed among objects when an object type is configured to have a parent of more than one type (typically, the second parent is a recursive object type).

For example, if Risk object types are configured to be a child of Process and a child of SubProcess object types, then a triangle relationship will exist among these different object types. [Figure 6 on page 72](#) shows an example of a triangle relationship between a child Risk and parent Process and Sub-Process object types.

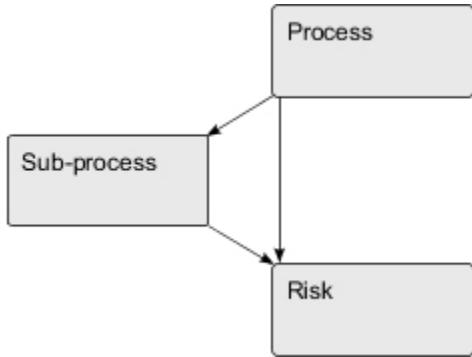


Figure 6. Triangle relationship between different object types

In the reporting framework, fields from parent objects within a triangle relationship (for example, Process and Sub-Process) are stored in the same Query Subject along with the ID of the shared child object (such as, Risk ID). When both Process and Sub-Process fields are part of the same Query Subject, a user would require Read permission on both Process and Sub-Process object types to view these fields in a report.

When a triangle relationship exists among objects, avoid the use of the Sub-Process (or similar) object type as a security point in your system unless you are willing to always grant Read access to the parent object type (such as Process).

Note: For information about configuring triangle object relationships in the reporting framework, see “[Triangle object relationships](#)” on page 801.

Sample scenario

A user has Read access for Sub-Process object types, so they can view details for Sub-Process objects in the application user interface.

If the same user does not have Read or Write access to the parent Process and Business Entity, that user will still have an implicit Navigate permission to the Process and Business Entity object types. The implicit Navigate permission allows users to navigate through the object hierarchy to object types that are lower in the hierarchy (such as Sub-Process) for which they have explicit permission (in this case, Read access).

If a triangle relationship exists among these object types, the same user would not have permission to view the Sub-Process detail in a report unless the user was also granted explicit Read access on the Process object type (as SUBPROCESSES and PROCESSES reside in the same Query Subject).

Security domains

In IBM OpenPages with Watson, special user groups, called "security domain groups", are automatically created when a Business Entity or Sub-entity object is created.

Security domain groups act as containers for users and organizational groups associated with that business entity.

In the > **Users and Security > Domains & Groups**, each security domain group is located under a top-level (root) **Security Domains** folder. The name of the group corresponds to the name of the business entity to which it belongs.

Users in a security domain group are generally assigned roles to work on the objects under that entity. You can also delegate specific security management activities to administrators in a security domain group for managing users and groups within that business entity.

Note: When you expand a security domain group folder, only child security domains are displayed. To view the organizational groups and users that are associated with the security domain, click the security domain group.

Example

You want to delegate the security activity of resetting passwords to an administrator for members of a particular Sales Office security domain group.

To do this, click the Sales Office security domain group. Add the administrator or click an existing administrator. Assign the "Reset Password" permission. That administrator can then reset passwords for users in that Sales Office security domain group only.

You could repeat this process of delegating "Reset Password" permission to an administrator for each security domain group within your organizational hierarchy.

Moving business entities

On occasion, you may need to reorganize your business entity structure by moving a Business Entity with its corresponding object hierarchy from one location to another.

When you move a business entity structure, all role assignments that were made on that business entity remain intact.

This means that users and groups who were granted various roles at a specific Business Entity security context point before the move operation, will continue to have the same roles and access after the move operation.

Note: If you are planning on moving a large object hierarchy, consider using the Entity Move/Rename utility that is included with IBM OpenPages with Watson. This utility allows batch processing of multiple Business Entities for overnight or weekend execution without running the risk of operations timing out. You can run the utility interactively or as a scheduled job. For more information, see the *Entity Move/Rename Utility ReadMe* and "[Entity Move/Rename utility](#)" on page 572.

Copying business entities

If you use the copy operation to expedite the setup of child business entities by duplicating an instance of an existing business entity, a security domain group for that new child business entity is automatically created by the system and is associated to the security domain group of the parent business entity.

Initially, the new security domain group that corresponds to the new child business entity is empty (no users or groups). However, users and groups who have assigned roles with access control defined for the parent business entity will have the same access on the new child business entity.

An administrator of the security domain group for the parent business entity can add and/or associate users and groups to the security domain group of the new child business entity. An administrator of the parent business entity can delegate administration activities by selecting an administrator. For details, see "[Delegate administrator permissions](#)" on page 42.

To refine user access to the new child business entity, you can use the application interface to define role templates and grant roles to users and groups. For details, see "[Role templates](#)" on page 75.

Role-based access control permissions

When you create a role template, you can specify the type of security access control that you want to have on an object type's folder structure for groups and users who are assigned to that role.

Note:

- The file (SOXDocument) and link (SOXExternalDocument) object types have the same root storage folder path. As a result, you can configure only one set of ACLs for both these object types in a role.
- Any new object types that are added to the system are excluded from all existing role templates.

Access control permissions for role-based security

For each object type that you want to include in a Role Template, you can set access control (ACL) permissions on the object's folder structure.

- **Read** - when you select an object type for inclusion in a role, the value of the Read permission is automatically set to Granted on the object's folder structure. This means that any groups or users assigned to this role can navigate to, and view the details of objects (parent and child) contained in the folder and the folder itself, but cannot modify any object data unless other permissions are explicitly set.
- **Write** - the groups or users assigned to this role can read and modify the details of objects within the selected folder, but cannot delete objects. Write access to a folder is required for creating new objects within the folder.
- **Delete** - the group or user assigned to this role can read, modify, and delete objects within the folder structure.
- **Associate** - the group or user assigned to this role can create associations between objects.

For each ACL permission, you can set an explicit value. These values or settings are propagated downward and inherited by any child object storage folders under that parent object's folder structure.

For each ACL permission, you can set one of the following values:

Note: For usage examples, see “[Scenarios: Using access control settings](#)” on page 74.

- **Unspecified** - by default, no access is explicitly granted to the user or group for the corresponding object through this role. The “Unspecified” setting does not override any access that is granted on this object through other roles or access inherited through a role on higher level security context points. This value should be used instead of “Denied” since it is less restrictive.
- **Granted** - this explicit setting gives a user or group full access to the specified action (Write/Delete/Associate). The user can modify, or delete the file or folder, depending on the permission.
- **Denied** - this explicit setting does not allow a user or group to perform the specified action (Write/Delete/Associate). The “Denied” setting overrides any access that is granted on this object through other roles or access inherited through a role on higher level security context points.

Scenarios: Using access control settings

The following case scenarios provide examples of how the system may respond with various settings.

Scenario 1: Using explicit settings

If a user or group is assigned multiple roles and the explicit ACL settings within these roles conflict, the most restrictive explicit setting will be used.

For example, we create a Test Performer and a Test Reviewer role for the Test object type. Each role has the **Write** ACL permission explicitly set to the following:

- Test Performer has **Write = Granted**
- Test Reviewer has **Write = Denied**

If we assign both roles (Test Performer and Test Reviewer) to a user called Tester1, Tester1 will not be able to create new Test objects even though the Test Performer role has Write = Granted. This is because the Write = Denied permission of the Test Reviewer role is more restrictive than the Write = Granted permission, and the most restrictive setting is automatically applied.

Scenario 2: Using explicit and unspecified settings

If a user or group is assigned multiple roles and one role has an explicit ACL settings but the other role has Unspecified for the same permission, the explicit setting will be used.

For example, we create an Initial Test and a Final Test role for the Test object type. The roles have the **Write** ACL permission set to the following:

- Initial Test has **Write = Granted**
- Final Test has **Write = Unspecified**

If we assign both roles (Initial Test and Final Test) to a user called Tester1, Tester1 will be able to create new Test objects even though the Final Test role has Write = Unspecified. This is because the Write = Granted permission is explicit and the explicit setting is automatically applied.

Scenario 3: Using unspecified settings

If a user or group is assigned a single role and the ACL settings within this role:

- Use the default value Unspecified, and
- No other access control has been explicitly set for the user or group

then access is DENIED.

For example, we create an Initial Test role for the Test object type. The role has the **Write** ACL permission set to the following:

Initial Test has **Write = Unspecified**

If we assign the role (Initial Test) to a user called Tester1 and Tester1 has not been granted access through any group-inheritance, Tester1 will not be able to create new Test objects.

Role templates

Role templates are global to the application and are available for role assignment by any administrator of a security domain who has the **Assign Roles** administrator permission.

Because the **Assign Roles** permission is a global permission, it is not constrained by the hierarchy of the role. Users who are granted this permission can manage any role in the system.

Role templates are the preferred method for granting users or groups application permissions.

Note:

- Both application permissions and ACLs are included in the role definition process. When a role is assigned to a user or a group on any business entity or security context point, that user or group automatically acquires the application permissions defined in that role template.
- When a user or group is assigned multiple roles, the user or group accumulates the application permissions that are defined in the various roles. Application permissions are granted by the role (not the security context point) and apply in all situations where the user has the correct ACL access. For example, users with Read permission to Business Entities and the **Audit Trail** application permission are able to view the **Activity** tab for those Business Entities.

Accessing Role Templates

You can define application permissions by using role templates.

Before you begin

Only a Super Administrator or a delegated administrator with the **Role Templates** permission can access Role Templates.

About this task

Procedure

1. Click  > **Users and Security** > **Role Templates**.
2. From the list of **Role Templates**, you can add, view, and modify role templates.

Adding a role template

You can add a role template to define application permissions.

Before you begin

Ensure that System Admin Mode is disabled.

About this task

The role template page guides you through creating a new role, selecting object types for inclusion or exclusion, and setting security on the selected object types.

Role template names are not localizable.

Note: Users who have roles that are assigned to a context security point within the Business Entity level only have only navigation access to the parent Business Entity. If users require the ability to view or modify the details of a parent Business Entity, then you must use an entity-based role template to grant explicit Read and/or Write permission to users at an entity security point.

Procedure

1. Click  > **Users and Security** > **Role Templates**.
2. Click **New Role Template**.
3. In **Name**, type a name for the role. For example, Tester01.
4. Optional: In **Description**, type a brief description of this role.
5. In **Role Type**, select the type of security context point you want from the list.

Note: If only one security context point type (such as Business Entity) is defined for your system, this is the only value in the list. Security context point types are derived from the security model that is in effect for your installation.
6. Click **Add**.
7. In the **Role Access Controls** section:
 - a) Click **Add** to assign object types to the role template.
 - b) Select the check box next to each object type for which you want to configure folder permissions.
For example, if you wanted to configure permissions for Risk and Issue objects, you would select *Risk* and *Issue*.

Note: Use Search, if needed. To select all object types, select the check box in the **Name** column.
 - c) Click **Add**.
After you assign the object type, you can assign permissions using a table format.
 - d) Click a row (or click the check box and click **Edit**) for an object type and select a setting value for each permission (Write, Delete, and Associate). By default, Read is always set to Granted, and all other permissions are set to Unspecified.
For setting details, see “[Role-based access control permissions](#)” on page 73.
 - e) Click **Done**. Repeat for other object types.
8. In the **Role Permissions** section:
 - a) Click **Edit**.
 - b) Select the application permissions that you want to assign to this role template. For a description of the various application permissions, see “[Types of application permissions](#)” on page 52.
 - c) Click **Done**.
The new role is listed on the **Role Permissions** section.
9. To assign the role to a user or group, see “[Assigning and removing a role from a user or group](#)” on page 78.

Modifying a role template

When you modify a role template after you assign it to users and/or groups, any changes you make to access control (ACLs) and application permissions are automatically propagated to those users and groups.

You can use this propagation feature to grant additional access control or revoke access control on certain object types to existing users and/or groups, by modifying the role template.

Typically, a Super Administrator or a top-level security domain administrator (with **Assign Roles** administration permission and **Role Templates** application permission) are able to modify, disable or delete a Role Template. This is because a lower-level security domain administrator, though having **Role Templates** application permission, does not have **Assign Roles** administration permission on higher-level entities and hence is not able to successfully edit, disable, or delete a template.

Procedure

1. Click  > **Users and Security** > **Role Templates**.
2. From the list of Role Templates, click the name of the role you want to modify.
3. Click **Edit**.
4. Make the required changes.
5. Click **Done**.

Enabling and disabling a role template

You can make a role inactive and keep it for future use by disabling the role. You can also enable a role that was previously disabled.

Procedure

1. Click  > **Users and Security** > **Role Templates**.
2. From the list of Role Templates, click the name of the role you want to enable or disable.
3. Click **Disable** or **Enable**.

Results

When you disable a role, the following occurs:

- Depending on the **Disable Role Group** application setting, any users and groups, who were previously assigned that role, either retain or lose their access control and application permissions. By default, the setting allows users and groups to retain access after a role is disabled. For more information, see ["Disable access control on Role groups" on page 501](#).
- The disabled role template is removed from the role assignment selection list and cannot be used for further role assignments.
- The status of the role on **Role Templates** changes from Active to Inactive.

When you enable a role, the following occurs:

- Any users or groups who are assigned that role are able to perform activities on objects that are associated with that role.
- The enabled role template is included in the role assignment selection list and can be used for further role assignments.
- The status of the role on **Role Templates** changes from Inactive to Active.

Deleting a role template

To automatically revoke all role assignments, you can delete a role template.

An administrator (or Super Administrator) with **Role Templates** application permission and the **Assign Roles** administrator permission can assign and/or revoke roles on any entity in the system. Only a Super Administrator or a top-level entity administrator is able to delete role templates, since this action automatically revokes all role assignments that were made using the selected role template on any business unit in the application.

When you delete a role, the following occurs:

- Any users or groups who were assigned that role are no longer able to perform the activities on objects that are associated with that role.
- The role is permanently removed from the list of roles on the **Role Templates** tab and cannot be restored.

If you want to remove a role without deleting it, you can disassociate the role instead by revoking the role from the user or group.

Procedure

1. Click  > **Users and Security** > **Role Templates**.
2. From the list of Role Templates, click the name of the role you want to delete. Click .

Assigning and revoking roles

An administrator of a parent domain group can assign or revoke roles only from its child groups and users.

For example, an administrator who has the **Assign Roles** administrator permission on a top-level a domain group can assign any role template to users and groups on that business entity or its child sub-entities.

If an administrator assigns a role template to a user or group on a security domain, the same access control that is granted on the corresponding business entity will be propagated to its child entities.

When an administrator assigns a role to a user or group on a lower-level domain that gives the user Read access to a lower-level business entity, the application provides the necessary access to navigate to that lower-level entity even though the user may not have Read access to all of its parent entities.

Example

You have a business entity with the following hierarchical structure:

Company ABC > North America > Boston

The business entity has the following processes:

Company ABC > North America > Boston > P1

Company ABC > North America > Boston > P2

If the administrator of the Boston office assigns a "Process Owner" role to user "Mary" granting Read access only to Processes associated with the Boston entity, then user "Mary" can navigate to processes associated with the Boston entity only, even though "Mary" cannot view the details of the entities Company ABC, North America and Boston.

Assigning and removing a role from a user or group

After role templates are created, you can assign one or more roles to groups and users on a security context point within a business entity security domain.

About this task

You can assign a role to a user or group by using the **Security Domains** page.

When you revoke a role from a user or group, the role assignment is explicitly removed from the user or group on a given entity.

Disassociating users from a security domain group does not result in removal of their role assignments on that entity.

You can revoke a role assignment from a user or group from the **Role Assignments** tab of the business entity security domain group page.

Alternatively, you can add and remove role assignments from the user account or the group. For more information, see [“Modifying user accounts” on page 49](#) and [“Creating an organizational group” on page 51](#).

Procedure

1. Click  > **Users and Security** > **Domains & Groups**.
2. Click **Domains**.
3. Click the name of the security domain group to which you want to add a role assignment for a user.
4. On the selected security domain group, go to the **Role Assignments** section.
5. Click **Add**.
6. In **User/Group**, find and select each group or user that you want to add.
7. In **Role Type**, select a security point. If only one security point (such as Business Entity) is defined for your system, this is the only value in the list.
8. Select a **Role Template**.
9. Click **Choose** next to **Security Domain**.
 - a) A list of security points is displayed. Expand the folder if needed.
 - b) Select one or more security context points from the list.
 - c) Click **Done**.
10. Click **Add**.
11. To remove a role assignment, go to the **Role Assignments** section. Select the user/group with a check mark and click **Remove**.

Viewing roles assigned to users or groups

You can use several methods to view which roles are assigned to users and groups.

- Run reports
- Open a user account and view role assignments. For more information, see [“Modifying user accounts” on page 49](#).
- Open a user or group and view a list of role assignments.
- Open a business entity security domain group and view a list of role assignments (described below).

Note: Role templates that were assigned directly to a parent or child business entity security domain group can only be viewed from the detail page of that parent or child. Role assignments that are made on a security domain are only displayed for that domain.

In the case of an extended security context model, for example, SOXBusEntity/SOXProcess or SOXBusEntity/SOXProcess/SOXSubprocess security models, role assignments on processes and subprocesses that are associated with the current security domain are also displayed. For more information, see [“Set the system security model” on page 500](#).

Procedure

1. Click  > **Users and Security** > **Domains & Groups**.
2. Click **Domains**.

3. Click the name of the business entity security domain group whose role assignments you want to view.
4. Go to the **Role Assignments** section.

Security rules

You can create two levels of security by using security rules:

- “[Record level security](#)” on page 81 allows administrators to control access to individual objects in a folder.
- “[Field level security](#)” on page 92 allows administrators to control access to individual fields within an object.

Security rules do not replace role-based security. Instead, they provide an extra level of security that can work with role-based security.

Consider this example of record level security. A folder contains 10 tasks. The role-based security grants the Read and Write access controls to all users in a certain role. You define a record level security rule to limit the access for one user who is in that role so that this one user has Read access for Task 1 and Task 8 only.

You can extend the example to field level security. Task 1 contains 10 fields. You can define a field level security rule to limit the access for one user in a certain role. This user has Read access for Field 3 and Field 7 only.

You define security rules for individual object types. After you have defined them, they are applied to all system components, including Reporting, FastMap, Triggers, Reporting Periods, and all available views.

A security rule comprises two parts:

- A formula that determines the conditions for granting the access controls.
 - The formula can be based on these field values: Actor fields, Enumerated fields, Text fields, Date fields, Numeric fields, and Currency fields.
 - The formula can be based on a user who is a member of particular user group or profile.
 - Complex formulae can be based on associations between objects.
- For example, a loss event is owned by the business unit where it occurred and is also shared with other business units that are impacted by the loss event. Selected users of the other business units should see its details.
- The formula can support complex expressions that use terms such as AND, OR, NOT, and nested parentheses.
- The access controls that specify the object access permissions or field access permissions.
 - A record level security rule can specify Create, Read, Update, Associate, and Delete access to object instances.
 - A field level security rule can specify Read only, and Read and Update access to non-system fields within an object.

A security rule formula has the following restrictions:

- They do not support computed text fields.
- They do not support long string fields.
- They do not support NULL values.

The NOT operator does not return objects that have an empty, blank, or null value in the selected field criteria.

- They do not support encrypted simple string or long string data type fields.
- When you use a Multi-Valued User/Group Selector in a security rule, the user or group that you specify in the formula must already exist in your environment.

- The functions that are used in security rule formulas are available in English only. For example, when you add a path to a security rule, the options in the **Parent or Child** list are in English only.

Note: Security rules are not applied to administrators. They have full permissions for all objects and fields.

Record level security

You can use record level security to control access to individual objects in a folder.

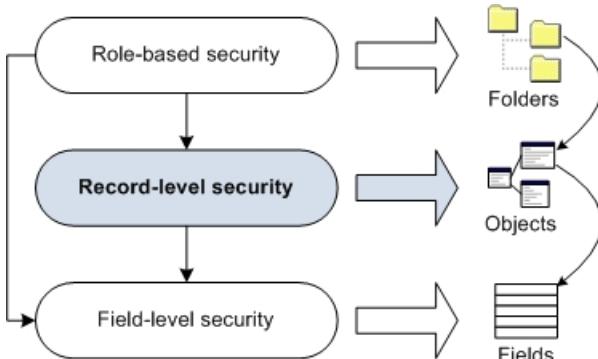


Figure 7. Record level security applies to objects

If no record level security is defined for an object, only role-based security is applied to the object.

When you define a record level security rule, the way that access is restricted depends upon whether the outcome of the formula is true or false when it is applied to an object:

- True: Access to the object is granted, and you can restrict or extend the existing role-based security for that object.
- False: Access to the object is not granted, and role-based security is applied.

When users view an object, they can see associated child objects only under the following circumstances:

- The associated child objects are included in a role template.
- The associated child objects are not included in a role template, but a record level security rule that extends role-based security is applied to the parent object.

RESTRICT and EXTEND rules

When you define a record level security formula, you define RESTRICT rules and EXTEND rules.

A RESTRICT rule is applied after role-based security (RBS). A RESTRICT rule further restricts access to an object. The following formula illustrates how a RESTRICT rule is evaluated:

```
If (RBS=True AND RESTRICT_RULE_RESULT=True), then grant access
```

Notice the AND operator. Role-based security must grant access, and the result of the RESTRICT rule must be true. The result is that users get access to the object if role-based security grants them access and the RESTRICT rule result is also true.

For example, suppose role-based security grants all users in the Finance group READ and UPDATE access on Control objects. But, you want users to be able to do an UPDATE only if they are also the owner of the control object. In this case, you can add a RESTRICT rule on UPDATE that checks the END_USER against the owner field of the object.

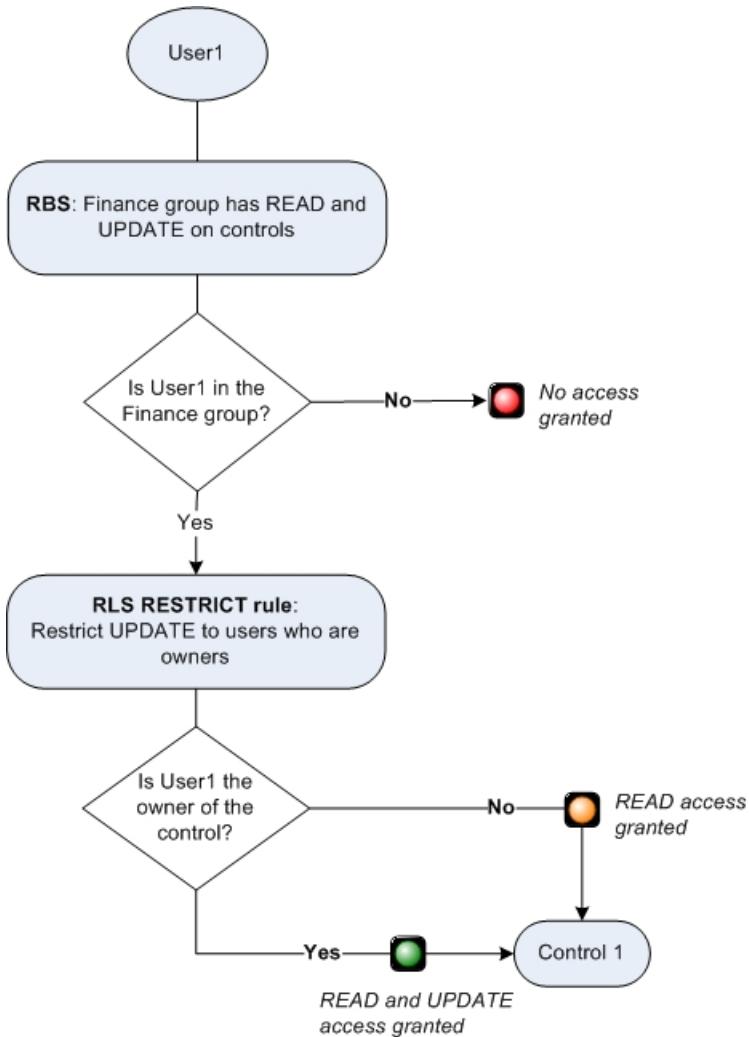


Figure 8. A RESTRICT rule grants UPDATE access if users are in the Finance group and are owners of the control

For a more detailed example, see the record level security scenarios, such as [“Scenario: Objects that are shared across GRC domains” on page 89](#).

An EXTEND rule is applied in addition to role-based security. An EXTEND rule grants access to an object for which role-based security does not grant access. The following formula illustrates how an EXTEND rule is evaluated:

```
If (RBS=True OR EXTEND_RULE_RESULT=True), then grant access
```

Notice the OR operator. Either role-based security must give access or the EXTEND rule result must be true. The result is that users get access to the object if role-based security gives them access or if the EXTEND rule result is true. Which means users gain access to the object in all of the following scenarios:

- Role-based security is granted and the EXTEND rule result is true, OR
- Role-based security is granted and the EXTEND rule result is false, OR
- Role-based security is not granted and the EXTEND rule result is true.

For example, suppose role-based security grants all users in the Finance group READ and UPDATE access on Control objects. However, you also want users to be able to READ and UPDATE if they are the owner of the control object, regardless of whether they belong to the Finance group. In this case, you can add an EXTEND rule on READ and UPDATE that checks the END_USER against the owner field of the object.

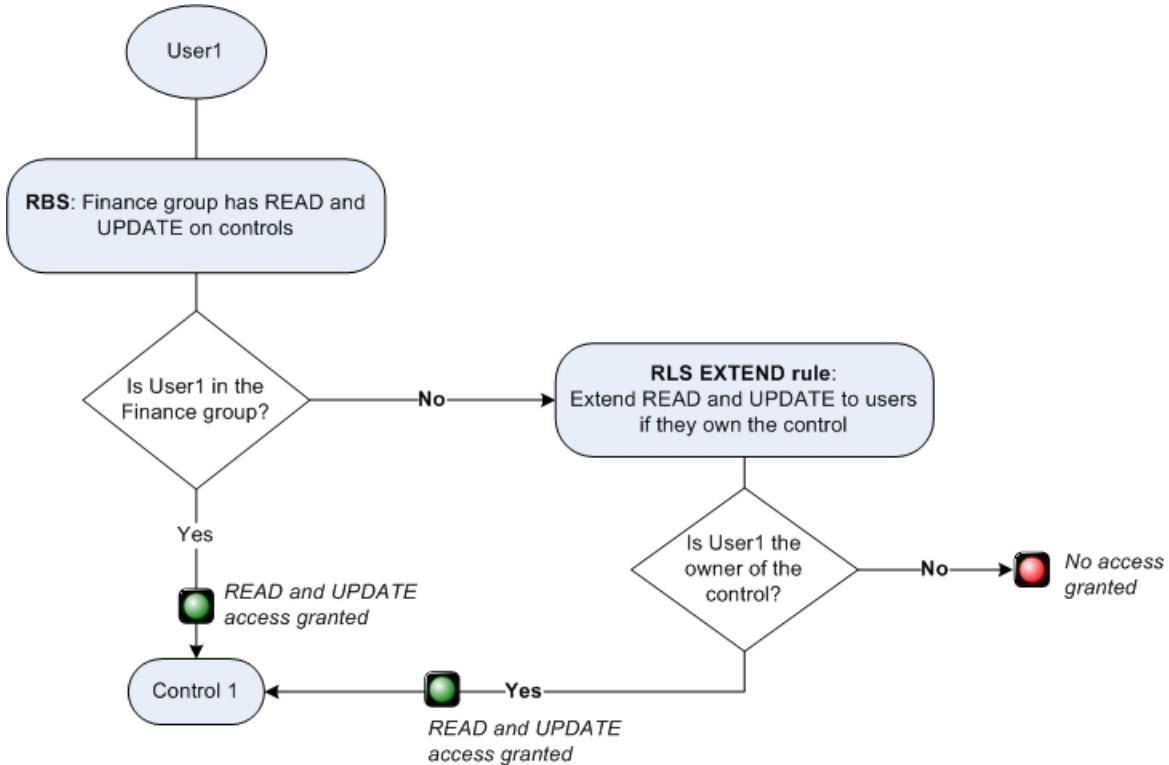


Figure 9. An EXTEND rule grants access to users who are owners of a control, regardless of their group membership

For a more detailed example, see the record level security scenarios, such as [“Scenario: Access for business administrators” on page 92](#).

Whether you are using a RESTRICT rule or an EXTEND rule, the rule is evaluated within the context of role-based security.

Multiple security rules

You can use multiple RESTRICT and EXTEND rules. Before you combine rules, ensure that you understand how security rules work in combination with each other. Incorrect assumptions about the behavior of security rules can lead to insecure models.

For each object type, you can have one record level security rule that grants READ access.

Combining RESTRICT rules

When you have multiple rules on the same object type with the same access, the rules are combined by using an OR expression.

Here is an example of two RESTRICT rules combined:

```

Restrict Rule 1 - Grants UPDATE
Restrict Rule 2 - Grants READ and UPDATE
  
```

Since each rule grants UPDATE access, the two rules are combined whenever the UPDATE access for a user needs to be determined. Each rule is evaluated on its own within the context of role-based security and access is granted if either of the rules evaluates to true. This means that the formula for this example is evaluated in the following manner:

```

If ((RBS=True AND RESTRICT_RULE_1_RESULT=True) OR
(RBS=True AND RESTRICT_RULE_2_RESULT=True)), then grant access
  
```

The result is that a user gets UPDATE access in the following scenarios:

- Role-based security is granted and the RESTRICT rule 1 result is true, OR

- Role-based security is granted and the RESTRICT rule 2 result is true.

Combining *RESTRICT* and *EXTEND* rules

You can combine RESTRICT rules with EXTEND rules. Each rule is evaluated within the context of role-based security, and then an OR condition is applied. However, do not combine RESTRICT and EXTEND rules on the same object for the same privilege.

For example, you can combine a RESTRICT rule for READ and UPDATE with an EXTEND rule for DELETE:

```
Restrict Rule on READ, UPDATE
Extend Rule on DELETE
```

The rules are evaluated in the following manner:

If evaluating READ access:

```
If ((RBS=True AND RESTRICT_RULE_RESULT=True), then grant access
```

If evaluating UPDATE access:

```
If ((RBS=True AND RESTRICT_RULE_RESULT=True), then grant access
```

If evaluating DELETE access:

```
If (RBS=True OR EXTEND_RULE_RESULT=True)), then grant access
```



Attention: Do not use the same access privilege in both rules. This can lead to results that might not be in-line with the behavior that you expect.

Here is an example of combined RESTRICT and EXTEND rules to help illustrate the point:

```
Restrict Rule on READ
Extend Rule on READ
```

The formula is evaluated in the following manner:

```
If ((RBS=True AND RESTRICT_RULE_RESULT=True) OR
(RBS=True OR EXTEND_RULE_RESULT=True)), then grant access
```

The result is that a user gets READ access in all of the following scenarios:

- Role-based security is granted and the RESTRICT rule result is true, OR
- Role-based security is granted and the EXTEND rule result is true, OR
- Role-based security is granted and the EXTEND rule result is false, OR
- Role-based security is not granted and the EXTEND rule result is true.

In other words, the user will have READ access with role-based security.

How combined security rules are evaluated

It is important to understand how RESTRICT rules and EXTEND rules are combined.

Many administrators assume that the EXTEND rule is evaluated after the RESTRICT rule, like this:

```
If ((RBS=True AND RESTRICT_RULE_RESULT=True) OR
EXTEND_RULE_RESULT=True), then grant access
```

The result would be that a user gets access in the following scenarios:

- Role-based security is granted and the RESTRICT rule result is true, OR
- The EXTEND rule result is true.

But this is not the case. Each rule is evaluated within the context of role-based security, and then an OR condition is applied:

Let's expand on this example to more clearly see the potential misunderstanding. Suppose that you have a user with the following set of circumstances:

- Role-based security access is granted to the user
- The RESTRICT rule for this user evaluates to FALSE
- The EXTEND rule for this user evaluates to FALSE

Using the formula from the assumed behavior the result of this scenario would be False:

```
((RBS=True AND RESTRICT_RULE_RESULT=True) OR EXTEND_RULE_RESULT=True) =  
((True=True AND False=True) OR False=True) =  
((True AND False) OR False) =  
(False OR False) =  
(False)
```

However, the formula that is actually being used is:

```
(RBS=True AND RESTRICT_RULE_RESULT=True) OR (RBS=True OR EXTEND_RULE_RESULT=True) =  
(True=True AND False=True) OR (True=True OR False=True) =  
(True AND False) OR (True OR False) =  
(False OR True) =  
(True)
```

Therefore, access would be granted for this user.

It is critical to understand how security rules work in combination with each other before you design your security framework. Incorrect assumptions on behavior can lead to insecure models.

Defining record level security rules

Use record level security rules to control access to individual objects in a folder.

Before you begin

You must enable System Admin Mode before you can define record level security. For more information, see [“Enabling and disabling System Admin Mode” on page 37](#).

Review the following information: [“Best practices for security rules” on page 102](#).

Procedure

1. Click  > **Users and Security** > **Security Rules**.
2. Click the name of the object type for which you want to define a security rule.
3. In the **Record Level Security Rules** section, click **Add**.
4. Add a name and description for the security rule.
5. In the **Security** property, specify how the security rule is combined with role-based security.
 - Select **Restrict** to apply both the role-based security and the security rule.
This option configures more restricted security. For example, if role-based security is set to **Read** and the security rule is set to **Update**, the **Restrict** setting provides read only access.
 - Select **Extend** to bypass role-based security when the outcome of the formula is true.
For example, if the role-based security is set to **Read** and the security rule is set to **Update**, the **Extend** setting allows a user to update information.
6. Set the **Status** of the security rule.
For more information, see [“Enabling or disabling a security rule” on page 101](#).
7. Specify the access controls.
For more information, see [“Minimum access controls for object operations” on page 87](#).

Note: Security rules for **Create** access are defined separately from rules for **Read**, **Update**, **Delete**, and **Associate** access. When you click **Create**, the other access options are unavailable.

Create

Users can create objects.

When a rule allows users to create objects, the formula cannot include fields within the object. It can include fields from the parent hierarchy, and other conditions that do not include fields. If you select **Create**, you cannot select any other access control for the rule.

Note: When you define record level security rules for the **Create** access control, use them only to further restrict role-based security.

You must use **Add Terms > Intended Parent** in the field when you use **Create**.

Read

Users can view the object.

If this option is unavailable, it means that the object type already has a READ rule enabled. You have the following options:

- Set the **Status** of the rule to **Disabled**. The **Read** option is then available. When you're ready to use the new READ rule, disable the existing READ rule first and then enable the new READ rule.
- Cancel and return to the list of security rules. Edit the existing READ rule to meet your requirements. For example, you can use the OR operator to set multiple conditions.

Update

Users can modify the object.

Delete

Users can delete the object.

Associate

Users can define associations or disassociations between objects.

When a rule allows users to associate objects, the formula cannot include fields within the target of the association. It can include fields from the child hierarchy, and other conditions that do not include fields.

8. Add the formula for the security rule.

You can type the formula or use **Add Path**, **Add Field**, and **Add Terms** to define parts of the formula. You can also use a combination of them. For more information, see “[Grammar for security rules](#)” on [page 98](#).

- a) To reference another object, either a parent or child, complete the following actions.

For more information, see “[Paths for parent and child objects](#)” on [page 95](#).

- i) Click **Add Path**.
- ii) Click **Parent or Child** and select whether the path follows parent objects or child objects.
- iii) Click **Starting Object Type** and select the object type that is the starting point for the path.
- iv) Click **Ending Object Type** and select the object type that is the ending point for the path.
- v) Click **Search** to view the possible paths.
- vi) Select one or more paths. If you select more than one path, use **Combine Paths** to specify how to use the multiple paths. Select **Any Path** if you want to use any of the paths or select **All Paths** if you want all paths to be used for the rule to be applied.

- vii) Click **Insert**.

- b) To define a field condition, complete the following actions.

For more information, see “[Terms for data types](#)” on [page 96](#).

- i) Click **Add Field**.
- ii) Select an object type.
- iii) Select the field that you want to use.
- iv) Select an operator. The list of operators changes depending on the field data type.

- v) Enter the value of the field condition.
- vi) Click **Insert** to add the field condition into the rule formula.

If you type the field condition, ensure that you use system names. If you do not specify an object type, the rule uses the object type for the object to which the rule applies. If you specify an object type, the object type must be either the subject of the rule or be specified in a path expression that contains the field reference.

You can use square brackets to ensure that when elements of field references contain spaces or other special characters, these field references are parsed.

- c) To add operators or keywords, click **Add Terms**.

9. Click **Validate**.

For more information, see [“Validating a formula for a security rule” on page 102](#).

10. Click **Add**.

11. Click **Show rule analysis**. Review the results and adjust the rule to reduce its performance impact.

For more information, see [“Best practices for security rules” on page 102](#).

You might see this message:

Multiple 'Read' rules can have a negative performance impact. They should be combined into a single rule.

Review the READ record level security rules for the object type. An object type can have only one READ rule enabled. Consider combining rules, for example:

```
(END_USER IN([SOXBusEntity].[OPSS-BusEnt].[Executive Owner])) OR  
(END_USER IN([SOXBusEntity].[OPSS-BusEnt].[Compliance Owner]))
```

What to do next

Test the security rule with a representative data set in a non-production environment. For example, test the grid views and reports that use the object types in the rule.

Minimum access controls for object operations

Users can perform the following operations on objects: Create, Read, Update, Associate and Delete. Each of these operations requires certain minimum access controls.

Create operation

The following table shows the minimum access controls that a user requires to create an object. Access controls are required for both the parent object and the child object.

Some access controls must be defined by using role-based security rather than record level security (as indicated in the table). In these instances, the access control for the parent object can be defined by using either type of security, but for the child object, it must be defined by using role-based security.

Table 47. Access controls required to create an object				
	Read	Write	Delete	Associate
Parent	Yes			Yes
Child	Yes (from role-based security)	Yes (from role-based security)		Yes (from role-based security)

Read operation

The following table shows the minimum access controls that a user requires to read an object.

These access controls can be defined in the role-based security or the record level security.

Table 48. Access controls required to read an object

	Read	Write	Delete	Associate
Object	Yes			

Update operation

The following table shows the minimum access controls that a user requires to update an object.

These access controls can be defined in the role-based security or the record level security.

Table 49. Access controls required to update an object

	Read	Write	Delete	Associate
Object	Yes	Yes		

Associate operation

The following table shows the minimum access controls that a user requires to associate an object.

Access controls are required for both the parent object and the child object.

Some access controls must be defined that use role-based security rather than record level security (as indicated in the table). In these instances, the access control for the parent object can be defined by using either type of security, but for the child object, it must be defined by using role-based security.

Table 50. Access controls required to associate an object

	Read	Write	Delete	Associate
Parent	Yes			Yes
Child	Yes (from role-based security)			Yes (from role-based security)

Delete operation

The following table shows the minimum access controls that a user requires to delete an object. Access controls are required for both the parent object and the child object.

These access controls can be defined in the role-based security or the record level security.

Table 51. Access controls required to delete an object

	Read	Write	Delete	Associate
Parent	Yes			Yes
Child	Yes		Yes	Yes

The following table shows the minimum access controls that a user requires to delete an object type that is self-contained or recursive, such as a Business Entity or Sub-Process. Access controls are required for both the parent object and the child object.

Some access controls must be defined using role-based security rather than record level security (as indicated in the table). In these instances, the access control for the parent object can be defined using either type of security, but for the child object, it must be defined using role-based security.

Table 52. Access controls to delete a self-contained object

	Read	Write	Delete	Associate
Parent	Yes			Yes

Table 52. Access controls to delete a self-contained object (continued)

	Read	Write	Delete	Associate
Child	Yes (from role-based security)		Yes (from role-based security)	Yes (from role-based security)

Scenario: Objects that are shared across GRC domains

Your company implemented the financial management and operational risk solutions. Because the teams that use these solutions share a common organizational hierarchy, they share some common object instances, such as processes. But they do not want to share other object instances, such as risks and controls.

Role-based security means that all users in the financial management and operational risk teams have access to all objects and object instances in the folder. Access controls need to be set for each domain so that users work with only the objects that they are responsible for. As well as securing objects, you are improving usability for your users.

For example, both of the financial management and operational risk teams use the Control object type but they use different instances of the Control object type. You want to enable users in the operational risk team to be able to update their instances of the Control object type. You also want to prevent users in the financial management team from viewing the instances that belong to the operational risk team.

You have two user groups for financial management and operational risk. Role-based security is already defined to grant **Read** and **Write** access controls to all users in the two teams. For example, a user in the SOXUsers group can update the controls that belong to the operational risk team.

Table 53. Permissions for each user group in the scenario

Domain	User Group	Permitted to work with	Not allowed to work with
Financial Management	SOXUsers	Compliance Controls	Operational Controls
Operational Risk	ORMUsers	Operational Controls	Compliance Controls

To satisfy the security requirements for these two user groups, role-based security is not changed. You add a security rule that further restricts the security that you already defined for the folder.

You define a security rule on the Control object type with the following information:

The formula is:

```
[SOXControl].[OPSS-Ctl].[Domain] IN ('Financial Management') AND END_USER IN GROUP('SOXUsers')
```

OR

```
[SOXControl].[OPSS-Ctl].[Domain] IN ('Operational Risk') AND END_USER IN GROUP('ORMUsers')
```

When the Security property is set to **Restrict**, both role-based security and the security rule are applied, and the Access controls are set to **Read** and **Update**.

Procedure

1. Click  > **Users and Security** > **Security Rules**.
2. Click the **Control** object type.
3. In the **Record Level Security Rules** section, click **Add**.
4. Add a name and description for the security rule.

5. In the **Security** property, select **Restrict** to have role-based security and the security rule both apply. **Restrict** prevents Compliance users from being able to view or work with the Operational Control.
6. Select the **Read** and **Update** access control check boxes.
7. Add the formula:
 - Click **Add Field** and select the **Control (SOXControl)** object.
 - Select the **Domain** field, and then select the Financial Management domain for the compliance team.
 - Click **Insert**.
 - Click **Add Terms** and select AND, then END_USER, and then IN GROUP.
 - Type 'SOXUsers'.

```
[SOXControl].[OPSS-Ctl].[Domain] IN ('Financial Management')
AND END_USER IN GROUP('SOXUsers')
```

- Repeat for the Operational Risk domain.
8. Click **Add**.

Scenario: Access to Issue Action Items

Issues that are created under one business unit can cause action items to be assigned to other lines of business. You need to ensure that all action item owners, regardless of business unit, can view the related issue.

An issue can have multiple action items that resolve the issue. The action items can be assigned to different business units and each business unit needs access to the issue object.

In this example, the compliance team has an Issue object that has two action items. One action item is for the compliance team. The other action item is for another business unit to complete some systems work.

Role-based security is set for the compliance team. They have access to all the objects in the folder, including the Issue object. A security rule is not required for the compliance team.

The other business unit needs access to the Issue object that is associated to the action item that they are responsible for. If you add the other business unit to role-based security, the other business unit has access to all objects in the folder. A security rule extends access to the other business unit for their action item and prevents them from working with other objects in the folder.

You define a security rule for the Issue object type with the following information:

The formula is:

```
FOR (Any Child [SOXIssue]/[SOXTask] : [SOXTask].[OPSS-AI].[Assignee] =
END_USER)
```

When the Security property is set to **Extend**, security is extended beyond role-based security. Users in the other business unit who are the owner of an action item that is associated with this issue can view the issue; however, they cannot view other issues that do not meet the criteria in the formula. The access controls are set to **Read**.

Procedure

1. Click  > **Users and Security** > **Security Rules**.
2. Click the **Issue** object type.
3. In the **Record Level Security Rules** section, click **Add**.
4. Add a name and description for the security rule.
5. In the **Security** property, select **Extend** to have the security rule extend the security that is set on the folder.
6. Select the **Read** access control.
7. Use **Add Path**, **Add Field**, and **Add Terms** to define the formula.

8. Click **Add**.
9. Click the **Task** object type.
10. In the **Record Level Security Rules** section, click **Add**.
11. Add a name and description for the security rule.
12. In the **Security** property, select **Extend** to have the security rule extend the security that is set on the folder.
13. Select the **Read** and **Update** access controls.
14. Use **Add Path**, **Add Field**, and **Add Terms** to define the formula.
15. Click **Add**.

Scenario: Security by job function

All auditors on the same team have the same profile, role template, and security context points. However, each auditor can have a different function for each audit. As an administrator, you want more flexibility in the way you apply security at the field level for each auditor.

This scenario is a variant of the scenario called *Lifecycle security*.

An auditor can have a different job function on different audits. For example, in Audit A, Jim is the lead auditor and can edit more fields than the other auditors.

Table 54. Audit A scenario		
Auditors	Job function	Permissions
Jim	Lead (In-charge)	<p>Jim can edit the Audit A instance of the Audit object and its descendants, Audit Sections, and Audit Workpapers.</p> <p>Jim's access controls are Create, Read, Update, and Associate.</p>
Susan	Field	<p>Susan can read and update specific areas of the Audit Sections and Audit Workpapers in the Audit A instance.</p> <p>Susan's access controls are Read and Update for these areas.</p>
Ellen	Field	<p>Ellen can read and update specific areas of the Audit Sections and Audit Workpapers in the Audit A instance.</p> <p>Ellen's access controls are Read and Update for these areas.</p>

However, in Audit B, Susan is the lead auditor while Jim is a field auditor.

Table 55. Audit B scenario		
Auditors	Job function	Permissions
Susan	Lead (In-charge)	<p>Susan can edit the Audit B instance of the Audit object and its descendants, Audit Sections, and Audit Workpapers.</p> <p>Susan's access controls are Create, Read, Update, and Associate.</p>

Table 55. Audit B scenario (continued)

Auditors	Job function	Permissions
Jim	Field	Jim can read and update specific areas of the Audit Sections and Audit Workpapers in the Audit B instance. Jim's access controls are Read and Update for these areas.
Ellen	Not involved in this audit	Ellen has no access controls set for her.

Scenario: Access for business administrators

Some users or groups need access to objects in a different way than most other users and groups in your organization. For example, business administrators need more access controls compared to other users, such as being able to update or delete an object.

This scenario is a variant of “[Scenario: Objects that are shared across GRC domains](#)” on page 89.

Exception management

One example is exception or waiver management.

In general, exceptions from a requirement, control, or process are granted on a project basis. The project is a child of a business entity and is implemented as a risk entity. The project can have secondary associations to a process, a subprocess, or a requirement. Exceptions are child objects of the project and define the requirement, control, or process from which the exception is seeking relief. The project is granted the exception. If no specific project is involved in the exception, the business entity is granted the exception.

All users can create exceptions but they can view only the exceptions that they created. The exception process custodians in IT have the job of reviewing and approving exceptions. You must extend role-based security to grant the exception process custodians in IT the ability to read and update all exceptions.

Privacy incidents

Another example involves the employees who are responsible for privacy incidents.

Specific individuals across the enterprise have responsibility for entering and maintaining information about Privacy incidents. In addition to other access that they have, they are designated as Privacy users and they might be in a Privacy Group or a Privacy Profile. The Privacy users can see all privacy incidents regardless of where the Privacy users are in the business hierarchy. They have access to additional fields on privacy incidents.

Similar functionality can be provided on other object types, such as audit findings, incidents, and waivers.

Scenario: All users can view objects and some users can update objects

Objects can be stored in a common area and shared across GRC domains. In this scenario, only a few users are allowed to update the objects. All other users have read access only.

This scenario is a variant of “[Scenario: Objects that are shared across GRC domains](#)” on page 89.

Role-based security is defined for all users to be able to read the objects in the folder. You want a small group to be able to create and another group to be able to update and associate.

Field level security

You can use field level security to control access to individual fields within an object. Field level security is applied to the set of objects that the user is entitled to by either role-based security or record level

security rules. If no field level security is defined for an object, security is applied at the object level (if security rules are defined) or at the folder level.

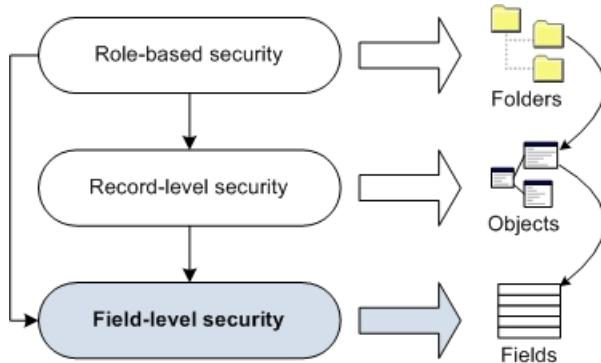


Figure 10. Field level security applies to object fields

When you define a field level security rule, you must consider all the scenarios that are required to access the field. If any scenarios are not defined, a user's access to the field is denied. This is known as redaction.

For example, one rule might specify that if a user is not an Owner, they have only Read access to a field. If a user is an Owner, they have Read and Update access. When the outcome of the formula is true, then Read access or Read and Update access is granted to a user. When the outcome of the formula is false, the field is redacted.

The way that access is restricted depends upon whether the outcome of a formula is true or false when it is applied to a field.

- True: The field is available to users as Read Only or Read and Update.
- False: The field is redacted. Users can see the field label, but not its value. Instead, the value is redacted, and the user sees some text, such as "Confidential" in place of the field value.

Restrictions:

- System fields are not supported.

The system fields are "Name", "Description", "Location", "Creation Date", "Created By", "Last Modification Date", "Last Modified By", and "Comment".

- Computed fields are not supported.
- Simple string fields that are encrypted are not supported.
- If more than one rule applies to a field, the rules are combined by using an OR condition.
- If more than one rule is defined for the same field, and one grants Read access to the field and another grants Read and Update access, then a user is granted Read and Update access if the outcome of the formula for each rule is true.
- Do not include fields that use field level security in Global Search. It might result in users being able to derive data values they otherwise would not have access to.

Redacted fields

When you define a field level security rule, if the outcome of the formula is false, the field is redacted. Users can see the field label, but not its value. Instead, the value is redacted, and the user sees some text, such as "Confidential" in place of the field value.

You can change the label of the text that is used to obscure the field value. For more information, see ["Localizing application text" on page 447](#).

Defining field level security rules

Use field level security to restrict access to specific fields within an object.

Before you begin

You must enable System Administration Mode before you can define field level security.

Procedure

1. Click  > **Users and Security** > **Security Rules**.
2. Click the name of the object type for which you want to define a security rule.
3. In the **Field Level Security Rules** section, click **Add**.
4. Add a name and description for the security rule.
5. Click **Choose Fields**, and select the fields on which to apply the security rule.
6. For each field that you selected, specify the access controls.

Read Only

Users can read the field values, but not update them.

Read and Update

Users can read and update the field values.

7. Add the formula for the security rule.

You can type the formula or use **Add Path**, **Add Field**, and **Add Terms** to define parts of the formula. You can also use a combination of them. For more information, see “[Grammar for security rules](#)” on [page 98](#).

- a) To reference another object, either a parent or child, complete the following actions.

For more information, see “[Paths for parent and child objects](#)” on [page 95](#).

- i) Click **Add Path**.
- ii) Click **Parent or Child** and select whether the path follows parent objects or child objects.
- iii) Click **Starting Object Type** and select the object type that is the starting point for the path.
- iv) Click **Ending Object Type** and select the object type that is the ending point for the path.
- v) Click **Search** to view the possible paths.
- vi) Select one or more paths. If you select more than one path, use **Combine Paths** to specify how to use the multiple paths. Select **Any Path** if you want to use any of the paths or select **All Paths** if you want all paths to be used for the rule to be applied.

- vii) Click **Insert**.

- b) To define a field condition, complete the following actions.

For more information, see “[Terms for data types](#)” on [page 96](#).

- i) Click **Add Field**.
- ii) Select an object type.
- iii) Select the field that you want to use.
- iv) Select an operator. The list of operators changes depending on the field data type.
- v) Enter the value of the field condition.
- vi) Click **Insert** to add the field condition into the rule formula.

If you type the field condition, ensure that you use system names. If you do not specify an object type, the rule uses the object type for the object to which the rule applies. If you specify an object type, the object type must be either the subject of the rule or be specified in a path expression that contains the field reference.

You can use square brackets to ensure that when elements of field references contain spaces or other special characters, these field references are parsed.

- c) To add operators or keywords, click **Add Terms**.
8. Click **Add**.
9. Click **Show rule analysis**. Review the results and adjust the rule to reduce its performance impact.
For more information, see “[Best practices for security rules](#)” on page 102.

What to do next

Test the security rule with a representative data set in a non-production environment. For example, test the grid views and reports that use the object types in the rule.

Paths for parent and child objects

There can be several paths between objects. For example, there might be two paths between Object A and Object D: A-B-D and A-C-D. When you define a security rule, you specify the starting point (Object A) and the end point (Object B) of the path. You then choose from a list of available paths.

To help you understand parent objects and child objects, consider the metaphor of a school. The students in the entire school can be thought of as having the role of any child. A classroom has a teacher, who can be thought of as the primary parent. The students in this classroom are the primary children of the teacher. Other teachers have the role of any parent. If you want to use the path from a teacher to the students in the teacher's classroom, you use **Primary Parent** or **Primary Child** as the path qualifier.

Parent objects

You can use the following parent objects in the path.

Primary Immediate Parent

Paths follow only to the lowest level primary parent. Use **Primary Immediate Parent** for recursive object types only.

Primary Parent

Paths follow only to the primary parent. There can be only one primary parent.

If a primary parent is specified, the path follows only primary parent relationships.

Any Immediate Parent

Paths follow only to the lowest level parent. Use **Any Immediate Parent** for recursive object types only.

Any Parent

Paths follow to any level of parent, such as grandparent or parent, within recursive object types. For example, a control has a parent that is a subprocess and the subprocess has a parent. When you use **Any Parent** in the path for the control, the parent can be the subprocess or the subprocess's parent.

Child objects

You can use the following child objects in the path.

Primary Immediate Child

Paths follow only to the immediate, highest level child or to the immediate primary child. Use **Primary Immediate Child** for recursive object types only.

Primary Child

Paths follow only to the primary child, which is a child of a primary parent. A primary parent can have several primary children. A child can have only one primary parent.

If a primary child is specified, the path follows only primary child relationships.

Any Immediate Child

Paths follow only to the immediate, highest level children, if the child is a recursive object type. Grandchildren are excluded.

Any Child

Paths follow to any level of child, grandchildren or children, within recursive object types.

Terms for data types

This list contains the data types, operators, keywords, and other terms that are supported in a security rule formula.

The following data types are supported:

- Boolean
- Integer
- Decimal
- Date
- Currency
- Simple string including all display types
- Enumerated (single-valued and multivalued)

Terms that can be used with all data types

The following terms are used with all data types.

AND

Narrows the search for objects. The objects must meet all of the criteria.

OR

Broadens the search for objects. The objects must meet one of the criteria, not all of them.

NOT

Narrows the search by excluding all objects that match the specified criteria.

() (parentheses)

Groups criteria together to show the order in which the rule is applied.

If parentheses are not used, the precedence rules are:

1. **NOT**
2. **AND**
3. **OR**

Terms that are used with numeric data types

The following operators are used with numeric data types, such as decimal, integer, and currency data types. Security rules do not support field criteria on computed text fields or large text fields.

= (equal)

Compares the values in two fields and returns "true" if both contain the same value.

< (less than)

Compares the values in two fields and returns "true" if the second field is less than the first field. The two fields must be of the same data type. For example, both are decimal data types.

> (greater than)

Compares the values in two fields and returns "true" if the second field is greater than the first field. The two fields must be of the same data type. For example, both are decimal data types.

<= (less than or equal)

Compares the values in two fields and returns "true" if the second field is less than or equal to the first field. The two fields must be of the same data type.

>= (greater than or equal)

Compares the values in two fields and returns "true" if the second field is greater than or equal to the first field. The two fields must be of the same data type.

< > (not equal)

Compares the values in two fields and returns "true" if both contain different values.

Uses string variables.

Terms that are used with string data types

The following operators are used with data types that require strings, such as enumerated strings and simple strings. Security rules do not support long strings.

CONTAINS

Determines whether a multiple-select field contains a specific value or set of values.

ENDS WITH

Determines if the field value ends with the specified text.

LIKE

Determines if a field value matches the specified pattern string.

STARTS WITH

Determines if the field value starts with the specified text.

IN

Determines if the field value is in the specified field.

Terms that are used with date data types

TODAY

Returns today's date.

TOMORROW

Returns tomorrow's date.

NOW

Returns the current date and time. You can specify a date or time in the future or in the past.

```
NOW(<integer>, {'<offset_type>'})
```

If you don't specify an `<offset_type>`, the default offset is used, which is days.

You can use the following syntax to specify the `<offset_type>`:

Table 56. NOW() syntax for offsets

To specify this...	Use
Years	'y' or 'year' or 'years'
Months	'm' or 'month' or 'months'
Weeks	'w' or 'week' or 'weeks'
Days	'd' or 'day' or 'days'
Hours	'h' or 'hour' or 'hours'
Minutes	'mi' or 'minute' or 'minutes'
Seconds	's' or 'second' or 'second'

For example:

- `NOW(5)` specifies a date five days from now.
- `NOW(2, 'm')` specifies a date two months from now.
- `NOW(-5)` specifies a date five days ago.
- `NOW(-2, 'y')` specifies a date two years ago.
- `NOW(2, 'h')` specifies a time two hours from now.

- NOW(-30, 'mi') specifies a time 30 minutes ago.

YESTERDAY

Returns yesterday's date.

DATE

Specifies the date and time as a string in the ISO format: YYYY-MM-DD and hh:mm:ss.sTZD.

You can also specify the date and its format as a string: DATE('09/05/2013', 'MM/dd/yyyy')

Terms that are used with other data types

END_USER

Returns the logged-in user.

END_USER_PROFILE

Returns the profile for the logged-in user.

IN GROUP

Returns the user group for the logged-in user.

IN PROFILE

Returns the specified field value that is in the specified profile.

INTENDED PARENT

Tests the parent under which a new object is to be created. It can be used only when you define a **Create** record level security rule.

Use **INTENDED PARENT** when you want to control what a user or group can create. For example, you can allow specific users to create risks for subprocesses but not for issues.

When you use **INTENDED PARENT**, the condition can depend on the object type that is referenced as intended parent. The condition can also depend on the object type of the security rule's subject. A path expression that uses intended parent is considered false if the intended parent is not of the specified object type.

Grammar for security rules

As an administrator, you need to understand the grammar for a security rule formula so that you understand the potential impact of adding a rule.

condition

Condition is the basic building block for a security rule formula.

```
|---- predicate -----+---|
 +-- NOT -- condition -----+
 +-- condition -- AND -- condition --+
 +-- condition -- OR -- condition --+
 +-- path-condition -----+
 '-- ( -- condition -- ) -----'
```

The following rule applies to condition:

- If parentheses are not used, the precedence rules are:
 1. NOT
 2. AND
 3. OR

path-condition

```
v----- AND -----.
>>-- FOR ( ---+--- path-direction -- path ---+--- : -- condition -- ) --<-
 | v----- OR -----. |
```

+--- path-direction -- path ---+
'-- intended-parent -----'

predicate

```
|---- scalar ---- = ----- scalar -----  
|      |  
|      +-- < -----  
|      +-- > -----  
|      +-- <= -----  
|      +-- >= -----  
|      '-- <> -----  
+-- like-predicate -----+  
+-- starts-with-predicate-----+  
+-- contains-predicate-----+  
+-- ends-with-predicate-----+  
+-- in-predicate -----+  
+-- in-group-predicate-----+  
'-- in-profile-predicate-----'
```

scalar-value

```
|---- field-reference -- +-+|  
|  +- end-user-profile -+-|  
|  +- boolean -----+|  
|  +- integer -----+|  
|  +- decimal -----+|  
|  +- date -----+|  
|  +- currency -----+|  
|  +- simple_string -----+|  
|  +- enum_value -----+|  
|  '- function -----'|
```

field-reference

```
>>-+-----+-- . -- field-group -- . . -- field-name --<<
     '-- object-type --'
```

The following rules apply to the field-reference:

- If no object-type is given, the object type is that of the object to which the rule applies.
 - If an object-type is given, it must either be the subject of the rule or been specified in a path expression that contains the field-reference.
 - All elements of the field reference must be system names.
 - Optional square brackets can be used to assure parsing in case elements of field references contain spaces or other special characters.

end-user-profile

```
|-- END_USER_PROFILE ( --+--- field-reference --+--- ) --|
   '-- string -----'
```

function

```
|----- TODAY -----+  
|   +- TOMORROW +  
|   +- NOW -+  
|       |   .-- ( 0, 'd' ) -+  
|       |   .-- , -- 'd' -+ .  
|   -- NOW -+- ( -- offset +-----+ ) -+-  
|           '--- , -+- 'y' -+-  
|               +- 'm' -+-  
|               +- 'd' -+-  
|               +- 'h' -+-  
|               +- 'mi' -+-  
|               '--- 's' ---'
```

like-predicate

```
|-- field-reference -- LIKE -- pattern-string --|
```

The following rule applies to the like-predicate:

- The pattern string must be a string constant.
- For information on what is supported for the like-predicate, see “[Limitations on special characters in filters for long string fields](#)” on page 205 and “[Using advanced logic in a search filter](#)” on page 210.

starts-with-predicate

```
|-- field-reference -- STARTS WITH -- string --|
```

contains-predicate

```
|-- field-reference -- ENDS WITH -- string --|
```

ends-with-predicate

```
|-- field-reference -- ENDS WITH -- string --|
```

in-predicate

```
|-- scalar-value -- IN ---+--- scalar-value -----+---|
|           |           v--- , -----.
|           |           -- ( --- scalar-value ---+--- ) ---|
```

The following rules apply to in-predicate:

- If a single field reference is given, it must be a multivalued field.
- If multivalued fields are used in the list, they are unnested.

in-group-predicate

```
|-- scalar-value -- IN GROUP ---+--- scalar-value -----+---|
|           |           v--- , -----.
|           |           -- ( --- scalar-value ---+--- ) ---|
```

The following rules apply to in-group-predicate:

- If a single field reference is given, it must be a multivalued field.
- If multivalued fields are used in the list, they are unnested.

in-profile-predicate

```
|-- scalar-value -- IN PROFILE ---+--- string -----+---|
|           |           v--- , -----.
|           |           -- ( --- string ---+--- ) ---|
```

The following rules apply to in-profile-predicate:

- If a single field reference is given, it must be a multivalued field.
- If multivalued fields are used in the list, they are unnested.

path

```
|-- object-type ----- v-----|  
      / -- object-type --+-|
```

path-direction

```
.-- ANY ----- .-- CHILD ---.  
|--- PRIMARY ---+-----+--- PARENT ---|  
     '-- IMMEDIATE --'
```

intended-parent

```
|-- INTENDED PARENT OF TYPE -- object-type -- |
```

Rules

- Combining multiple paths with AND or OR is semantically equivalent to specifying multiple path expressions with the same condition combined by AND or OR.
- For combined paths, the end point of all paths in the path expression must have the same object type. The condition can contain references only to the shared starting points and ending points as well as any references to outer paths that lead up to the subject.
- A path expression for a given path of object types is considered true if the condition is true for any instantiation of the path.
- Except for combined paths described earlier, the condition can depend on any object type along the path of the path-expression.
- The condition may also depend on object types along the path of containing path-expressions or the subject object type of the rule.
- When using intended-parent, the condition can depend on the object-type referenced as intended parent as well as the subject object-type of the rule. A path expression that uses the intended parent clause is considered false if the intended parent is not of the specified object-type or the operation is not Associate or Create.
- Depending on the path-direction specified, the path lists a connected series of object types relative to the current context either following parent or child relationships.
- The outermost path must start with the rule's subject type. Nested paths must start with the endpoint of the immediately containing path.
- If IMMEDIATE is specified and the end point of the path is a recursive object type, the path stops at the bottom most parent of that type or the top most child.
- If PRIMARY is specified, the path will follow only primary parent relationships.

Enabling or disabling a security rule

You can work on a security rule without making it available to your users. When the security rule is ready, you can enable it. Conversely, you can withdraw a security rule by disabling it so that you can make all required changes to it.

Before you begin

You must enable System Admin Mode before you can work with security rules. For more information, see [“Enabling and disabling System Admin Mode” on page 37](#).

Procedure

- Click  > **Users and Security** > **Security Rules**.

2. Select the object type that contains the security rule that you want to enable or disable.
3. Click the check box of the rule, and then click **Enable** or **Disable**.

Note: You can enable only one READ record level security rule for an object type.

Validating a formula for a security rule

When you validate a formula for a security rule, IBM OpenPages with Watson checks the completeness of the formula that you entered and verifies that the syntax of the rule is correct.

Note: The validation is validating only whether the rule is syntactically correct. It does not validate whether the values are valid. The values that you provide are validated when you save.

For example, in the following expression, the left side of the equation shows an enumerated string field. The right side has a Boolean value. The syntax would be correct if the status field was Boolean. The validation does not recognize that the data types are different.

[SOXIssue] . [OPSS-Iss] . [Status] = FALSE

Before you begin

You must enable System Admin Mode before you can work with security rules. For more information, see [“Enabling and disabling System Admin Mode” on page 37](#).

Procedure

1. Click  > **Users and Security** > **Security Rules**.
2. Select the object type that contains the security rule that you want to validate.
3. Click the name of the security rule.
4. Click **Validate** for the formula that you want to validate.
5. When you see a message that the formula has successfully validated, click **Done**.

Deleting a security rule

When a security rule is no longer required, you can delete it. You cannot undo the deletion.

Before you begin

You must enable System Admin Mode before you can work with security rules. For more information, see [“Enabling and disabling System Admin Mode” on page 37](#).

Procedure

1. Click  > **Users and Security** > **Security Rules**.
2. Select the object type that contains the security rule that you want to delete.
3. Click the check box of the rule, and then click **Delete**.

Best practices for security rules

When you configure security rules, consider the following best practices.

Analyzing security rules

Use **Show rule analysis** to gain insights into the potential performance impact of your security rules. The analysis includes all rules that are enabled for an object type. The analysis is broken down by rule type (record level security or field level security) and by access control.

Click  > **Users and Security** > **Security Rules**, click an object type, and then click **Show rule analysis**. Review the information to understand the impact of the security rules on performance.

Tip: If the **Show rule analysis** button is not available, open a rule, make a change, and then click **Save**.

<i>Table 57. Metrics for security rules analysis</i>	
Metric	Description
Fields evaluated	The total number of fields that the rules need to evaluate. Keep the number of fields low.
Total hierarchy walks	The number of different object type hierarchies that the rules need to use. For example, a rule for the Issue object type might extend Update access if the current user is assigned to a child action item. In this example, the rule is using two object type hierarchies: one for Issues and one for Action Items. Keep the number of hierarchies low.
Total hierarchy levels	The total number of hierarchy levels across all the object types that the rules use. For example, a rule for the Issue object type might evaluate the Action Items that are children of the issue. In this example, the number of hierarchy levels is 1. Keep the number of levels low.
Navigating object hierarchy using ANY	The number of times the rules use an ANY function, such as Any Parent or Any Child to evaluate a path. Consider whether you can use a more specific function. For example, if you're using Any Parent, consider whether you can use Any Immediate Parent or Primary Parent instead. The goal is to reduce the number of possible parents or children that a rule needs to consider.
Navigating down the object hierarchy	The number of times the rules must evaluate downward in the object hierarchy. For example, a rule for the Issue object type might evaluate the Action Items that are children of the issue. In this example, the rule is moving down the hierarchy to a child object, Action Item. Moving downward in a hierarchy can have a performance impact because each object instance can have many children, each of which a rule must evaluate. For example, a Control can have many child Issues, which in turn can have many child Action Items.
Multi-Value fields evaluated	The number of multi-valued fields that the rules need to evaluate. Multi-valued fields include enumerated string fields, Multi-Valued User, Multi-Valued Group, and Multi-Valued User/Group selector fields.
Group fields evaluated	The number of user fields and group fields that the rules need to evaluate. For example, a rule on a Control might check if the current user is a member of a group. In this example, the rule is using one group field. For a list of the user and group fields, see “Defining user/group fields” on page 173 .
Extend	Indicates whether the object type has any Extend rules. In general, Extend rules have a greater impact on performance than Restrict rules.

Creating rules for file attachments

You can create rules that extend or restrict access to file attachments. The object type for file attachments is SOXDocument. However, the SOXDocument object type is also used by system files, such

as FastMap templates. When you create a rule on SOXDocument, you need to ensure that users can still access the system files.

For example, suppose that users in the Policy group need access to file attachments where the document type is Policy Attachment. But you also need to ensure that all users can access the FastMap export template. You need to create a formula with two clauses: one to grant all users access to the FastMap template and another to grant the Policy group access to the file attachments they need.

```
[SOXDocument].[System Fields].[Location] STARTS WITH '/Templates/FastMap/%'  
OR ([SOXDocument].[OPSS-File].[Document Type] IN ('Policy Attachment')  
AND END_USER IN GROUP ('Policy'))
```

Combining record level security rules for an object type

If you have a (Create) and (Read or Associate) rule for an object type, you must add an extra OR condition to the (Read or Associate) rule. This condition is required so that the (Create) and (Read or Associate) rules can work together.

The OR condition looks like this:

```
(NOT(FOR (Any Parent [Rule_ObjectType]/PATH : 1=1))  
AND [Rule_ObjectType].[System Fields].[Created By] = END_USER)
```

Where:

- Rule_ObjectType is the object type in which the Read rule is created.
- PATH is the path of the Read rule, starting from the Rule_ObjectType.

The following example shows the security rule for LossEvent to control the Read operation for LossEvents under BusinessEntity.

```
OR (NOT(FOR (Any Parent [LossEvent]/[SOXBusEntity] : 1=1))  
AND [LossEvent].[System Fields].[Created By] = END_USER)
```

Lifecycles

You can use security rules with lifecycle triggers.

Security rules are evaluated before lifecycle triggers and actions modify an object. If an object's state before the lifecycle trigger meets the record level security criteria, you can update the object. The lifecycle trigger might modify fields so that the object state no longer meets the record level security rules.

If you use lifecycle triggers, consider using workflows or calculations instead. For more information, see [Chapter 16, “Configuring GRC Workflow,” on page 369](#) and [Chapter 15, “Configuring GRC Calculations,” on page 327](#).

Encryption

IBM OpenPages with Watson supports the following optional features:

- You can configure a custom encryption key to encrypt passwords that are stored in OpenPages properties files.

If you do not configure a custom encryption key, the passwords in properties files are still encrypted. However, your organization policies might require you to use a custom encryption key.

- You can encrypt specific fields in the IBM OpenPages with Watson repository to prevent system administrators from viewing confidential data directly from the database.

Create a keystore

You can create a keystore for IBM OpenPages with Watson.

Create the encryption keystore file and key pair

Before you can set up the encryption keystore in IBM OpenPages with Watson, you must create an encryption keystore file that contains the key pair details.

The file must use the Java format (jceks). Although you can use any keytool to create the file, it must use the same format as a Java keystore.

The encryption key must use one of the following encryption algorithms. Any other algorithms are not supported.

Table 58. Supported encryption algorithms

Algorithm name	Key size
3DES	168
AES128	128
AES192	192
AES256	256

When you run the keytool -genseckekey command, you are prompted for the keystore password and the key password.

Important: You must use the same password for the keystore and the key.

In the following example, the command generates a keystore that uses the supported Java format (jceks). The encryption key uses a 3DES encryption algorithm with a key size of 168.

```
keytool -genseckekey -alias openpages -keyalg 3DES -keysize 168  
-storetype jceks -keystore keystore-3DES.jks
```

In the following example, the command generates a keystore that uses the supported Java format (jceks). The encryption key uses an AES encryption algorithm with a key size of 256.

```
keytool -genseckekey -alias openpages -keyalg AES -keysize 256  
-storetype jceks -keystore keystore-AES256.jks
```

Setting up the encryption keystore

The encryption keystore is a file that stores the key that you use to encrypt passwords that are stored in properties files and to encrypt data in the IBM OpenPages with Watson repository.

Before you begin

You need a keystore file and you need to know the keystore password. For more information, see [“Create the encryption keystore file and key pair” on page 105](#).

Procedure

1. Enable System Admin Mode.

For more information, see [“Enabling and disabling System Admin Mode” on page 37](#).

2. Click  > **Users and Security** > **Encryption Keystore**.

3. Click **Edit**.

4. Enter the name of the encryption key in the **Key Name** field.

5. Enter the alias in the **Key Alias** field.

Important: Ensure the alias that you specify is an exact match to the alias in the keystore file.

6. Enter the keystore location in the **Keystore Location** field.

For security reasons, you cannot browse to the location, you must type it manually.

7. Select the encryption algorithm that is used by the key in the **Algorithm** field.

8. Enter the keystore password in the **Keystore Password** field,

Important: Ensure the password that you specify here is an exact match to the password in the keystore file.

9. Confirm the password in the **Re-enter Keystore Password** field.

10. Enter a description for the keystore in the **Description** field.

11. Click **Update**.

Note: If you change any of these keystore properties in future, you must update the keystore. For more information, see [“Updating the encryption keystore” on page 111](#).

Configure a custom encryption key for passwords in properties files

You can configure a custom encryption key to encrypt the passwords that are stored in properties files.

Note: If you already configured a custom key but the properties of the key changed, see [“Updating the encryption keystore” on page 111](#).

You need to do the following tasks to use a custom key to encrypt passwords that are stored in property files:

- Create a file that contains the encryption keystore and key pair. See [“Create the encryption keystore file and key pair” on page 105](#).
- Set up the encryption keystore. [“Setting up the encryption keystore” on page 105](#)
- Create a **keystore.properties** file. See [“The keystore.properties file” on page 106](#).
- Update the property files on all application servers to use the custom encryption key. See [“Updating property files on application servers to use a custom key” on page 107](#).
- Update property files on all reporting servers to use the custom encryption key. See [“Updating property files on reporting servers to use a custom key” on page 108](#).
- If you use global search, update property files on the search server to use the custom encryption key. See [“Updating property files on the search server to use a custom key” on page 109](#).

The **keystore.properties** file

Create a **keystore.properties** file. The file defines the custom encryption key to use for passwords that are stored in IBM OpenPages with Watson properties files.

Do this task after you create a keystore and configure it in IBM OpenPages with Watson.

Use the following text as a template:

```
#Tue December 13 23:35:46 EDT 2018
key.password=<password for the encryption key>
key.alias=<alias (name) of the encryption key>
keystore.path=<full path to the .jks file>
store.password=<password for the keystore>
```

Note: The **key.password** and the **store.password** must be the same.

For the **keystore.path** parameter, use a directory that all of your application servers and reporting servers can access. If you use global search, ensure that your search server can also access the directory. You have the following options:

- Specify a network location that all application servers, reporting servers, and the search server can access.
- Or, store the **.jks** file in the same directory on each server.

- Or, create a `keystore.properties` file for each type of server.

Example:

```
#Tue December 13 23:35:46 EDT 2018
key.password=password
key.alias=openpages
keystore.path=C:\\\\admin\\\\keystore-AES128.jks
store.password=password
```

Updating property files on application servers to use a custom key

After you configure a custom encryption key, update the property files on your application servers to use the custom encryption key.

Before you begin

The following tasks must be completed before you begin:

- Create a file that contains the encryption keystore and key pair. See “[Create the encryption keystore file and key pair](#)” on page 105.
- Set up the encryption keystore. “[Setting up the encryption keystore](#)” on page 105
- Create a `keystore.properties` file. See “[The keystore.properties file](#)” on page 106.
- Verify that all application servers can access the `keystore.path` that is specified in the `keystore.properties` file.

Procedure

1. Stop all OpenPages application servers, admin and non-admin.

See “[Stopping application servers](#)” on page 711.

2. Copy the `keystore.properties` file to the `<OP_HOME>/aurora/bin` directory.

3. Edit the `aurora.properties` file.

- a) Go to the `<OP_HOME>/aurora/conf` directory.
- b) Make a backup copy of the `aurora.properties` file.
- c) Open the `aurora.properties` file in a text editor.
- d) Change the following password values after the equal sign to plain text.

```
security.system.password=<openpages_system_password>
database.PASSWORD=<openpages_db_password>
```

- e) Save and close the file.

When you restart the servers later in this task, the passwords are re-encrypted with the custom encryption key.

4. Edit the `aurora_auth.config` file.

- a) Go to the `<OP_HOME>/aurora/conf` directory.
- b) Make a backup copy of the `aurora_auth.config` file.
- c) Open the `aurora_auth.config` file in a text editor.
- d) Locate the `security.search.user.credentials` parameter
- e) Change the value after the equal sign to plain text.
- f) Save and close the file.

When you restart the servers later in this task, the password is re-encrypted with the custom key that you specified.

5. Edit the `bootstrap.properties` file.

- a) Go to the `<OP_HOME>/wlp/usr/servers/<server_name>Server<#/>` directory.

- b) Make a backup copy of the bootstrap.properties file.
- c) Open the bootstrap.properties file in a text editor.
- d) Change the following password value after the equal sign to plain text.

```
op.jdbc.password=<jdbc_password>
```

- e) Save and close the file.

When you restart the servers later in this task, the passwords are re-encrypted with the custom encryption key.

6. Edit the op-backup-restore.env file.

- a) Go to the <OP_HOME>/aurora/bin directory.
- b) Make a backup copy of the op-backup-restore.env file.
- c) Open the op-backup-restore.env file in a text editor.
- d) Change the following password values after the equal sign to plain text.

IBM Db2

DB_OP_PWD: Type the password of the schema owner for the OpenPages database.

Oracle

- DB_SYSTEM_PWD: Type the password of the SYSTEM user for the OpenPages database.
- DB_SYS_PWD: Type the password of the DBA user for the OpenPages database.
- DB_OP_PWD: Type the password of the schema owner for the OpenPages database.

- e) Save and close the file.

7. Re-encrypt the passwords in the op-backup-restore.env file with the custom encryption key that you specified.

- a) Go to the <OP_HOME>/aurora/bin directory.
- b) Run the following command:

Windows

```
OPBackup.cmd secure
```

Linux

```
./OPBackup.sh secure
```

- c) Open the op-backup-restore.env file in a text editor and verify that the passwords are encrypted.

8. If you are using a horizontal cluster, do steps 2-6 on each application server in the cluster.

9. Start all OpenPages application servers, admin and non-admin.

See “[Starting application servers](#)” on page 709.

Results

The passwords are encrypted with the custom encryption key that you specified in the keystore.properties file.

Updating property files on reporting servers to use a custom key

After you configure a custom encryption key, update the property files on your reporting servers to use the custom encryption key.

Before you begin

The following tasks must be completed before you begin:

- Create a file that contains the encryption keystore and key pair. See “[Create the encryption keystore file and key pair](#)” on page 105.
- Set up the encryption keystore. “[Setting up the encryption keystore](#)” on page 105
- Create a `keystore.properties` file. See “[The keystore.properties file](#)” on page 106.
- Verify that all reporting servers can access the `keystore.path` that is specified in the `keystore.properties` file.

Procedure

1. Copy the `keystore.properties` file to the `<CC_HOME>/tools/bin/` directory.
2. Edit the `op-cc-backup-restore.env` file.
 - a) Go to the `<OP_HOME>/tools/bin` directory.
 - b) Make a backup copy of the `op-cc-backup-restore.env` file.
 - c) Open the `op-cc-backup-restore.env` file in a text editor.
 - d) Change the following password value after the equal sign to plain text.

```
DB_CC_PWD=<cognos_db_password>
```

 - e) Save and close the file.
3. Re-encrypt the passwords in the `op-cc-backup-restore.env` file with the custom encryption key.
 - a) Go to the `<CC_HOME>/tools/bin` directory.
 - b) Run the following command:

Windows

```
OPCCBackup.cmd secure
```

Linux

```
./OPCCBackup.sh secure
```

- c) Open the `op-cc-backup-restore.env` file in a text editor and verify that the password is encrypted.
4. If you are using a horizontal cluster, update each reporting server in the cluster.

Results

The passwords are encrypted with the custom encryption key that you specified in the `keystore.properties` file.

Updating property files on the search server to use a custom key

If you use global search, update the property files on your search server to use the custom encryption key.

Before you begin

The following tasks must be completed before you begin:

- Create a file that contains the encryption keystore and key pair. See “[Create the encryption keystore file and key pair](#)” on page 105.
- Set up the encryption keystore. “[Setting up the encryption keystore](#)” on page 105
- Create a `keystore.properties` file. See “[The keystore.properties file](#)” on page 106.
- Verify that the search server can access the `keystore.path` that is specified in the `keystore.properties` file.

Procedure

1. Copy the `keystore.properties` file to the `<SEARCH_HOME>` directory.
2. Disable global search and stop the global search services.
See “[Stopping the global search services by using a script](#)” on page 713 or “[Stopping the global search services](#)” on page 715.
3. Open a shell or command window as an administrator and then go to the `<SEARCH_HOME>` directory.
4. Run the following command to encrypt the password with the custom key:

Tip: You do not need to change the password. You can use the same value for the `<old_op_db_password>` and `<new_op_db_password>` parameters.

```
java -jar opsearchtool.jar setdbuserpassword -username <op_db_username>
      -password <old_op_db_password> -newusername <op_db_username> -newpassword
      <old_op_db_password>
```

You do not need to change the global search service (Apache Solr) password. The global search service password is stored in a registry setting, not in a properties file.

5. Start the global search services.

See “[Starting the global search services by using a script](#)” on page 712. Or if you want to start global search as a service, see “[Starting the global search services on Windows](#)” on page 713 or “[Starting the global search services on Linux](#)” on page 714.

Results

The password that the search server uses to access the database server is encrypted with the custom encryption key that you specified in the `keystore.properties` file.

Configure field level encryption

You can encrypt specific fields in the IBM OpenPages with Watson repository to prevent system administrators from viewing confidential data directly from the database. Data in encrypted fields is shown as a string of random characters.

Simple string and long string field data types are supported.

Fields that are encrypted are not eligible for use in Global Search.

Note: Before encrypting long strings in OpenPages running on Oracle 12.2, refer to the following Technote: <http://www.ibm.com/support/docview.wss?uid=swg22010106>. The Technote describes a potential issue and how to resolve it by obtaining the appropriate patch from Oracle support and applying it to your environment. The IBM OpenPages with Watson reporting framework handles encrypted fields by running a database function to decrypt them. When a long string (CLOB) field is made encrypted, the framework must be regenerated to call this database function. For more information, see “[Generating the reporting framework](#)” on page 814.

Restrictions:

- The maximum size of long strings that can be encrypted is 2 MB.
- Do not include encrypted long string fields in the search criteria for a filter because they can return unexpected results.

You need to do the following tasks to use field level encryption:

- Create a file that contains the encryption keystore and key pair. See “[Create the encryption keystore file and key pair](#)” on page 105.
- Set up the encryption keystore. “[Setting up the encryption keystore](#)” on page 105
- Place the keystore file on the application servers in your environment.

In a horizontal environment, the keystore file must be available to each application server. There are two options:

- Each application server must have access to the file location on the admin application server.
 - The file must be available in the same location on each application server.
- In a non-clustered environment, place the keystore file on the admin application server.
- Enable the keystore. See “[Enabling the encryption keystore](#)” on page 111.

Note: If you already configured field level encryption but the properties of the key changed, see “[Updating the encryption keystore](#)” on page 111.

Enabling the encryption keystore

After you set up the encryption keystore, you must enable it to encrypt the IBM OpenPages with Watson repository. If required, you can disable the keystore later to decrypt the repository again.

About this task

When you enable the keystore, any fields that are currently marked for encryption are automatically encrypted in the repository. If there are no fields that are marked for encryption, the keystore is enabled, meaning that it is ready to automatically encrypt any fields that are marked for encryption from now. For information on marking fields for encryption, see “[Encrypting field values](#)” on page 163.

Procedure

1. Click  > **Users and Security** > **Encryption Keystore**.
2. Click **Enable**.

Depending on the size of the repository, encryption can take a long time. Encryption runs as background event. You can view the progress by clicking **Refresh**.

Disabling the encryption keystore

After the IBM OpenPages with Watson repository is encrypted, you can disable the keystore to decrypt the repository again.

About this task

When you disable the keystore, any fields that are currently marked for decryption are automatically decrypted in the repository. If no fields are marked for decryption, the keystore is disabled, meaning that it is ready to automatically decrypt any fields that are marked for decryption from now. For information on marking fields for decryption, see “[Decrypting field values](#)” on page 164.

Procedure

1. Click  > **Users and Security** > **Encryption Keystore**.
2. Click **Disable**.

Depending on the size of the repository, decryption can take a long time. Decryption runs as background event. You can view the progress by clicking **Refresh**.

Updating the encryption keystore

Your company IT policy might require that you periodically change the encryption key. Whenever the encryption key details change, you must update the encryption keystore in IBM OpenPages with Watson.

Note:

If field level encryption is already enabled, you do not need to disable the encryption keystore to update it.

Procedure

1. Create a new keystore file.

For more information, see “[Create the encryption keystore file and key pair](#)” on page 105.

2. Create a `keystore.properties` file. See “[The keystore.properties file](#)” on page 106.

3. Click  > **Users and Security** > **Encryption Keystore**.

4. Click **Edit**.

5. Enter the current encryption keystore password to access it.

6. Update the details of the keystore.

For more information, see “[Setting up the encryption keystore](#)” on page 105.

7. Click **Update**.

If you use field level encryption and it is enabled, the fields are re-encrypted using the new encryption key. Depending on the size of the repository, updating the encryption can take a long time. Field encryption runs in the background. You can view the progress by clicking **Refresh**.

8. Update passwords in properties files.

- a) On each application server, change the passwords in properties files to plain text, save the files, and then restart the application server.

For more information, see “[Updating property files on application servers to use a custom key](#)” on page 107.

- b) On each reporting server, change the passwords in properties files to plain text, save the files, and then restart the reporting server.

For more information, see “[Updating property files on reporting servers to use a custom key](#)” on page 108.

- c) If you use global search, change the passwords in properties files to plain text, save the files, and then restart the server.

For more information, see “[Updating property files on the search server to use a custom key](#)” on page 109.

The passwords are encrypted with the updated encryption key when you restart the servers.

9. If you use IBM OpenPages Loss Event Entry, re-enter the password for each locale.

- a) Start the configuration tool. Go to `http://<server_name>:<port>/openpages/app/jspview/lossevent#/editconfig`

- b) Log in with a user account that is a member of the OPAdministrators group.

- c) Under the **Locales** section, expand each locale and enter the password.

- d) Close the configuration tool.

The passwords are encrypted with the updated encryption key.

10. If you use LDAP for user provisioning, do the following steps:

- a) Click  > **Users and Security** > **User LDAP Configuration**.

- b) Edit the LDAP configuration.

- c) In the **Security credentials** field, re-enter the password that is used to authenticate with the LDAP server.

- d) Click **Save**.

The security credentials are encrypted with the updated encryption key.

11. If you use natural language classifiers, do the following steps:

- a) Click  > **Integrations** > **Mapping and Taxonomy Suggestions**.

- b) Edit the classifier configuration.

- Natural Language Classifier: In the **API Key** field, re-enter the API key of the Natural Language Classifier instance.

- Watson Discovery Analyze API: Re-enter the password.
- c) Click **Save**.
- d) Repeat these steps for each classifier configuration.

The API keys are encrypted with the updated encryption key.

LDAP user authentication

IBM OpenPages with Watson supports the use of an LDAP (Lightweight Directory Access Protocol) authentication server to control user access.

To use LDAP user authentication, you integrate OpenPages with Watson with an LDAP data source.

Only one login module can be active at the same time. OpenPages with Watson supports a single namespace. All users must be authenticated through the same data source. Multiple authentication modules can be used in a multi-forested environment.

Users that are created or imported into OpenPages with Watson must also be defined in the LDAP authentication server. The administrator managing the OpenPages with Watson users is responsible for maintaining the correlation between the OpenPages with Watson user list and the external LDAP data source. If a user is disabled on the OpenPages with Watson server, the user must be manually disabled on the LDAP Directory server.

Note: If an LDAP Directory server is being used for user authentication, the **Change Password** option is disabled in OpenPages with Watson. When an LDAP server is used, passwords are not maintained in OpenPages with Watson. The password must be changed in the LDAP server.

You can also configure OpenPages with Watson to use an external LDAP user authentication server over SSL. For more information, see [“Modifying the LDAP configuration file for LDAP over TLS” on page 669](#).

Configuring the LDAP Authentication Module

To successfully use an LDAP Directory Server with IBM OpenPages with Watson, you must configure the LDAP Authentication Module to recognize the presence of the LDAP server.

To configure OpenPages with Watson to work with an external LDAP authentication source, complete the following tasks:

- [“Adding existing users to the LDAP server” on page 113](#)
- [“Modifying the LDAP configuration file” on page 114](#)

Adding existing users to the LDAP server

You can add existing IBM OpenPages with Watson users to an LDAP server.

Make sure to refer to your LDAP Directory Server documentation for the steps required to add users to the LDAP server.

Important: If you are using Microsoft Active Directory Users and Computers as your LDAP authentication server, the user name is limited to 20 characters. User names that exceed the 20-characters limit are truncated to 20 characters. This length limitation does not occur in the LDAP server provided by Sun.

All users that require access to the OpenPages with Watson application or server platform must be added to the LDAP authentication server. In addition, the following users will need to be added to the LDAP server:

- OPSystem

Note: If you specify a password for the OPSystem account that is different from the one installed by the product, you will need to complete [“Changing the OPSystem password” on page 637](#) to change the OPSystem account password system-wide.

- The OpenPages with Watson Super Administrator (for more information, see [“The Super Administrator” on page 41](#))
- OPAdministrator (only if you are using this account)

Modifying the LDAP configuration file

You must modify the authentication configuration file to enable the LDAP Directory Server that you are using.

Note: If you are using LDAP over SSL, see [“Modifying the LDAP configuration file for LDAP over TLS” on page 669](#).

The `aurora_auth.config` file contains three authentication modules:

- Openpages - the default internal user directory
- OpenpagesIP - a sample LDAP configuration for the Sun One Directory Server
- OpenpagesAD - a sample LDAP configuration for the Microsoft Active Directory Server

The only module that the IBM OpenPages with Watson system pays attention to is the module that is named Openpages. Therefore, you need to make a backup of the Openpages module, rename the OpenpagesIP or OpenpagesAD to Openpages, and then change the settings to reflect the settings of your LDAP server.

Procedure

1. Stop all OpenPages with Watson services.
2. Open and edit the `<OP_Home>/aurora/conf/aurora_auth.config` file in a text editor.

Where:

`<OP_Home>` is the installation location of the OpenPages with Watson application.

3. Find the Openpages module and change its name to `OpenpagesDefault`.
4. Modify either the `OpenpagesIP` or `OpenpagesAD` module name to `Openpages`.
 - If you are using a Microsoft Active Directory server, change the name of the `OpenpagesAD` module to `Openpages`.
 - If you are using a Sun One Directory Server, change the name of the `OpenpagesIP` module to `Openpages`.
 - If you are using a different LDAP server, you can use either of these modules. Choose a module to use as a template and change its name to `Openpages`.
5. Specify the correct values for the following properties in the module that you named `Openpages`:

provider.url

Change the value to the hostname and port number for the LDAP authentication server. For LDAP, the protocol is `ldap` and the port is the LDAP port number (by default, 389).

base.dn

The top level of the LDAP directory tree structure (Domain Name) on the LDAP server. If the users to be authenticated are located in multiple locations within your Active Directory structure, list all of the locations explicitly by using the distinguished names of the locations, each separated by a semi-colon.

For example:

```
base_dn="DC=LDAPTesting,DC=local,CN=Users,DC=LDAPTesting,DC=local;
OU=Auditors,OU=External Auditors,OU=Staff,DC=LDAPTesting,DC=local"
```

user.attr.id

The attribute name of the user identifier (for example, `uid`, `cn`, etc.)

Additional custom parameters

You can add additional custom parameters that are supported by the Java Naming and Directory Interface (JNDI). Precede a JNDI property with the `ctx.env.` prefix.

For example, if you want to use the JNDI property `com.sun.jndi.ldap.connect.timeout`, use `ctx.env.com.sun.jndi.ldap.connect.timeout=<value>` in the `aurora_auth.config` file.

For information about JNDI properties, see the [Java SE documentation](http://docs.oracle.com/javase/7/docs/technotes/guides/jndi/jndi-ldap.html#JNDIPROPS) (<http://docs.oracle.com/javase/7/docs/technotes/guides/jndi/jndi-ldap.html#JNDIPROPS>).

For example:

```
Openpages
{
    com.openpages.aurora.service.security.namespace.LDAPLoginModule
        required debug=false
        provider.url="ldap://myserver.company.com:389"
        security.authentication="simple"
        security.search.user.dn="cn=Directory Manager"
        security.search.user.credentials="openpages"
        base.dn="ou=people,o=IBM,c=US"
        user.attr.id="uid"
    ;
}
```

6. When you are finished editing the file, save your changes and exit.

7. Restart all services.

Results

You have configured the OpenPages with Watson system to use an external LDAP user authentication server.

Setting up mixed-mode authentication

Use mixed-mode authentication when not all users can use a single namespace for authentication.

This solution should be used by customers who do not want to create the OPSSystem, SOXAdministrator, OpenPagesAdministrator, or OPAdministrator user accounts on their LDAP server but do want all their users to be authenticated by LDAP. The following procedure creates a new namespace and modifies user names (such as OPSSystem) to authenticate against the OpenPages with Watson authentication module rather than LDAP.

Procedure

1. To create the namespace modules in the `aurora_auth.config` file, log on to the application server.
2. Find and open the `aurora_auth.config` file.
3. Create or update the namespace modules in the file as follows:

```
OpenpagesDefault
{
    com.openpages.aurora.service.security.namespace.AuroraLoginModule
        required debug=false;
}

Openpages
{
    com.openpages.aurora.service.security.namespace.LDAPLoginModule required
        debug=false
        provider.url="ldap://192.168.0.169:30429"
        security.authentication="simple"
        base.dn="DC=LDAPTesting,DC=local;OU=People,DC=LDAPTesting,DC=local"
        user.attr.id="uid"
```

```
};
```

4. To create the namespace in the database, log on to the database instance with the database id, such as OPENPAGES.
5. Run the following SQL to create the OpenpagesDefault namespace:

```
insert into namespaces (NAMESPACEID, NAME, JAASLOGINMODULE, DESCRIPTION) values (namespaceidseq.nextval, 'Openpages Security', 'OpenpagesDefault', 'Default Openpages Security Namespace');
```

6. Run the following SQL to point an ID to the new namespace:

```
update actors set namespaceid = (select namespaceid from namespaces where JAASLOGINMODULE = 'OpenpagesDefault') where actorid = (select actorid from actorinfo where name = 'user_name');
```

For example, the following SQL will have the OPSSystem use the OpenpagesDefault namespace for authentication:

```
update actors set namespaceid = (select namespaceid from namespaces where JAASLOGINMODULE = 'OpenpagesDefault') where actorid = (select actorid from actorinfo where name = 'OPSystem');
```

7. Commit the changes to the database.

Configuring a multi-forested LDAP authentication

IBM OpenPages with Watson supports the use of multiple LDAP authentication servers in a multi-forested configuration. If the application cannot find the user in the first authentication server, it will check the next server in the list and repeat until it finds the user or checks all listed authentication servers.

When listing multiple LDAP servers, the `aurora_auth.config` file must be modified to contain multiple sets of server information.

This file is located in the `<OP_Home>\aurora\conf` directory, where `<OP_Home>` is the installation location of the OpenPages with Watson application. By default, this is `c:\OpenPages`.

This is accomplished by grouping the server information by index key, as in the following example:

```
com.openpages.aurora.service.security.namespace.LDAPLoginModule required
debug=true
provider.url.1="ldap://10.128.22.106:389"
security.authentication.1="simple"
security.search.user.dn.1="CN=Administrator,CN=Users,DC=parent,DC=parentchild,DC=localdomain"
security.search.user.credentials.1="0p3nPag3s"
base_dn.1="DC=parent,DC=parentchild,DC=localdomain"
user.attr.id.1="CN"
provider.url.2="ldap://10.128.22.107:389"
security.authentication.2="simple"
security.search.user.dn.2="CN=Administrator,CN=Users,DC=child,DC=parent,DC=parentchild,DC=localdomain"
security.search.user.credentials.2="0p3nPag3s"
base_dn.2="DC=child,DC=parent,DC=parentchild,DC=localdomain"
user.attr.id.2="CN"
```

By adding a ".1" key to the end of each parameter, OpenPages with Watson can parse the settings correctly and differentiate between separate LDAP server information sets. You would append a ".2" to the keys for the second LDAP server, and so on.

For single LDAP server implementations, you do not need to append an identifier to the end of the parameter names.

Chapter 7. Managing the reporting schema

The IBM OpenPages with Watson application supports the use of a real-time reporting schema model that allows reports to access information as it is entered into the system. Data does not need to be exported to an external reporting database repository.

See “[Changes that require the reporting schema to be updated or re-created](#)” on page 117 for a list of tasks that require the reporting schema to be re-created. The OpenPages with Watson application does not have to be restarted after re-creating the reporting schema.

Changes that require the reporting schema to be updated or re-created

You can update the reporting schema or re-create it when necessary.

For more information, see “[Updating the reporting schema](#)” on page 121.

The following table lists the tasks that require the reporting schema to be re-created and the tasks where you can opt to update the reporting schema instead. In some cases, the reporting framework must also be regenerated.

This type of change lists tasks. **Requires this action** has the following nested columns:

- **Generate reporting schema**

If **Yes**, indicates that you must re-create the reporting schema after doing the task.

- **Update reporting schema**

If **Yes**, indicates that you can do an update rather than re-creating the reporting schema. Because an update of the reporting schema allows for incremental changes to the reporting schema, there is no need to re-create it. However, if you prefer, you can re-create the reporting schema instead of updating it.

- **Generate reporting framework**

If **Yes**, indicates that the reporting framework needs to be regenerated after you do the task.

Table 59. Re-creating the reporting schema and regenerating the reporting framework			
This type of change...	Requires this action...		
	Generate reporting schema	Update reporting schema	Generate reporting framework
Adding a new field to a field group.	No	No	Yes
Adding a new object type.	No	No	Yes
Adding a new association between object types.	No	No	Yes
Removing object types or attributes.	Yes	No	Yes
Encrypting a long string (CLOB) field.	No	No	Yes
Defining, modifying, or deleting business entity recursive object levels.	No	No	Yes
Removing a field from a field group.	No	No	Yes
Disabling an association between object types.	No	No	Yes

Table 59. Re-creating the reporting schema and regenerating the reporting framework (continued)

This type of change...	Requires this action...		
	Generate reporting schema	Update reporting schema	Generate reporting framework
<p>Changing the security model.</p> <p>Note: Changing the security model after data is loaded or migrated into the system is not recommended and requires assistance from the OpenPages Support team.</p>	Yes	No	Yes
<p>Changing the value of the Populate past periods setting.</p> <p>For more information, see “Populating past reporting periods” on page 119.</p>	Yes	No	No
<p>Changing any setting used to compose URL links in the reporting schema, for example, the Host, Port, and Protocol settings.</p> <p>To update the reporting schema by running the RPS_Update SQL script, see “Updating URL host pointers for reports” on page 633. To update the reporting schema by using the UI, see “Updating the reporting schema” on page 121.</p>	Yes	No	No
<p>Adding an index to an RT_column by using the Settings > Platform > Reporting Schema > Create Index on Fields setting.</p>	No	Yes	No
<p>Setting or changing the display type of a field to Multi-Valued User Selector or Multi-Valued Group Selector or Multi-Valued User Group Selector.</p>	No	Yes	No
<p>Importing a profile by using ObjectManager or the Import Configuration feature.</p>	No	Yes	No
<p>Configuring the triangles setting. For more information, see “Triangle object relationships” on page 801.</p>	Yes	No	No

Other situations that require the reporting schema to be created, re-created, enabled, and disabled are described in the *IBM OpenPages with Watson Installation and Deployment Guide*.

For more information, see “[Creating or re-creating the reporting schema](#)” on page 120. It is a good idea to schedule this activity ahead of time because creating a reporting schema requires that the application be in System Admin Mode. In this mode, users are not able to log on to the system and users who are currently logged in are not able to commit changes to the repository.

Note: Depending on your changes, re-creating the reporting schema and regenerating the reporting framework for Cognos reports might not cause your modifications to appear in the standard reports. You

might also need to modify your existing reports or create new reports to display the additional information (such as adding new fields).

Populating past reporting periods

You can control whether data from previous reporting periods or the current reporting period is included in the reporting schema.

Use the following procedure to change the **Populate Past Periods** setting, which controls what is populated in the reporting schema. By default, the reporting schema is populated with the data from previous reporting periods.

Procedure

1. Click  > **System Configuration** > **Settings**.
2. Expand the **Platform | Reporting Schema** folder hierarchy.
3. Click the **Populate Past Periods** setting.
4. In the **Value** field, type one of the following values:

Table 60. Past period reporting values

Value	Description
true	<p>The reporting schema is populated with the data from the current reporting period and all past reporting periods that are enabled.</p> <p>This value is set by default.</p> <p>Note: When this setting is set to true, it increases the amount of data that is published by the Reporting Schema operation and increases the time it takes to drop and re-create the Reporting Schema.</p>
false	The reporting schema is populated with the data from the current reporting period.

5. Click **Done**.

What to do next

Re-create the reporting schema (see, “[Changes that require the reporting schema to be updated or re-created](#)” on page 117).

Reporting schema permissions

Before performing any actions on a reporting schema, you must have specific application permissions set on your account.

The Reporting Schema task is used to control the creation and deletion of the reporting schema. Administrative-level users who have the Reporting Schema application permission can access the task.

For more information, see “[Types of application permissions](#)” on page 52).

Table 61. Reporting schema and framework permissions

This application permission...	Is used to...
Reporting Schema	<ul style="list-style-type: none">Access the  > System Configuration > Reporting Schema menu item.
System Administration Mode	Enable and disable System Admin Mode.

Creating or re-creating the reporting schema

You can create, re-create, enable, and disable a reporting schema. You can also drop reporting schema tables to reclaim database space.

Before you begin

The system must be in System Administration Mode (see [“Enabling and disabling System Admin Mode” on page 37](#)) to modify the reporting schema.

Ensure that no reports, backups, or other jobs are running. Do not run any reports, backups, or other jobs during the schema creation process.

Check the setting that controls whether past reporting periods are included in the reporting schema. For more information, see [“Populating past reporting periods” on page 119](#).

About this task

Creating a new reporting schema automatically enables the reporting schema, while dropping the reporting schema automatically disables it.

When the reporting schema is enabled, the database tracks changes to the application data and allows the reporting engine to access the updated data. When the schema is disabled, the database no longer tracks changes to the application data, but is still aware of changes to the schema (such as new fields).

The system keeps a log of each reporting schema operation that has been performed.

Note: You can also create or re-create the reporting schema by using the command line. For more information, see [“Generating the reporting schema and framework from a command line” on page 121](#).

Procedure

1. Enable System Admin Mode (SAM). Click  > **Enable System Admin Mode**.
2. Click  > **System Configuration** > **Reporting Schema**.
3. To create or re-create a reporting schema, perform one of the following actions:
 - If a reporting schema already exists, click **Re-CREATE** to drop the existing schema and create a new schema.
 - If no reporting schema exists, click **Create**. The new reporting schema is automatically enabled.
4. To enable the reporting schema, click **Enable**.
5. To disable the reporting schema, click **Disable**.
6. To reclaim the database space taken by the reporting schema tables, click **Drop**. This automatically disables the reporting schema.

What to do next

To view details of a reporting schema operation and review errors, use search to find the operation you want to view. A summary page opens with two tabs, **Information** and **Log**.

When the creation task (or re-creation task) is complete, update the Reporting Framework so that the Cognos reports can access the new schema. For more information, see [“Updating the reporting framework” on page 817](#).

Updating the reporting schema

Update the reporting schema.

Before you begin

Ensure that no reports, backups, or other jobs are running. Do not run any reports, backups, or other jobs during the schema update process.

About this task

When you update the reporting schema, any custom indexes you previously defined are automatically re-created by using the latest definition that is found in the appropriate registry entry. This capability is enabled by default, but it can be disabled. For more information about the settings for creating indexes, see the *IBM OpenPages with Watson Administrator's Guide*.

Procedure

1. Log in to OpenPages as a user with administrative privileges.
2. Click  > **Enable System Admin Mode**.
3. Click  > **System Configuration** > **Reporting Schema**.
4. Click **Update**.
5. Click **Refresh** until the process is 100% complete.
6. Disable SAM. Click  > **Disable System Admin Mode**.

Generating the reporting schema and framework from a command line

You can generate the reporting schema and the reporting framework by using the RpsRpF.sh | .cmd tool from a command line.

Before you begin

- JAVA_HOME must be set.
- The client tools must be installed. For more information, see [“Installing tools and utilities \(IBM OpenPages with Watson\)” on page 692](#) or [Installing tools and utilities in Cloud Pak for Data](#).
- If you are creating or re-creating the reporting schema, ensure that no reports, backups, or other jobs are running. Do not run any reports, backups, or other jobs during the schema creation process.

About this task

You can use the RpsRpF.sh | .cmd tool to create the reporting schema, the reporting framework, or both. When you generate the reporting framework, all framework models are generated.

You must have the following application permissions:

- **API > Administration > Background Process > Get Process Info**
- To create or re-create the reporting schema, you must be a super administrator. Or, you must have these permissions:
 - **Administration > System Administration Mode**
 - **SOX > Administration > Reporting Schema**
- To generate the reporting framework, you must be a super administrator. Or, you must have this permission:
 - **SOX > Administration > Reporting Framework**

Procedure

1. Go to the directory where client tools are installed:

IBM OpenPages with Watson

Go to the `<OP_HOME>/bin` directory on the application server.

Or, if you installed the client tools on a remote system, go to the `openpages-tools-client/bin` directory. The computer must be able to communicate with the OpenPages application server.

IBM OpenPages for IBM Cloud Pak for Data

Go to the `openpages-tools/bin` directory on the remote system where you installed the client tools package. The remote system must have access to IBM OpenPages for IBM Cloud Pak for Data.

2. Verify the properties in the `openpages-tools-client.properties` file.

IBM OpenPages with Watson

Verify that `rest.url.path` is set to the base URL of the public REST API on the application server, for example: `https://<host>:<port>/grc/api`

IBM OpenPages for IBM Cloud Pak for Data

- Verify that `rest.url.path` is set to the base URL of the public REST API, for example `https://<cpd_url>/openpages-<instance_name>-grc/api`

Replace `<cpd_url>` with the URL of IBM Cloud Pak for Data. Replace `<instance_name>` with the name of the OpenPages instance.

- Verify that `platform.cloudpак.jwt.auth` is set to `true`.

3. Open the `RpsRpf.properties` file.

4. Set credentials in the properties file

IBM OpenPages with Watson

```
OPENPAGES_ADMIN_USERNAME=
OPENPAGES_ADMIN_PASSWORD=
```

IBM OpenPages for IBM Cloud Pak for Data

```
OPENPAGES_JWT_USER=
OPENPAGES_JWT_TOKEN_OR_API_KEY=
```

5. Set the following parameters:

RPSRPF_ACTION_TYPE

- RPS: Create the reporting schema.
- RPF: Generate the reporting framework.
- BOTH: Create the reporting schema, and then generate the reporting framework.

DROP_REPORTING_SCHEMA

Optional. If you want to drop the reporting schema and re-create it, change `DROP_REPORTING_SCHEMA` to `true`.

Note: Do not modify `RPF_PARAMS`.

The following example shows a properties file for IBM OpenPages with Watson. With this configuration, the tool creates the reporting schema and then generates the reporting framework.

```
# OpenPages Administrator account
OPENPAGES_ADMIN_USERNAME=OpenPagesAdministrator
OPENPAGES_ADMIN_PASSWORD=
#JWT Auth
OPENPAGES_JWT_USER=
OPENPAGES_JWT_TOKEN_OR_API_KEY=
# Action type
# RPS - Reporting Schema Creation
# RPF - Reporting Framework Generation
```

```
# BOTH - Both RPS and RPF ( default )
RPSRPF_ACTION_TYPE=both

# Comma-separated reporting Framework options. Default is all options for v6 schema
RPF_PARAMS=dimensionFacts,customQuerySubjects,genType_6,i18NTranslationType_6
# Uncomment the next line for V5 Reporting Framework
#RPF_PARAMS=dimensionFacts,customQuerySubjects,genType_552,i18NTranslationType_552

# Drop reporting schema when it creates one
DROP_REPORTING_SCHEMA=false
```

Note: The V5 Reporting Framework is no longer supported. Do not uncomment the V5 Reporting Framework line.

6. Run the `RpsRpf.sh| .cmd` tool:

Windows

Open a command prompt as an administrator, and then run the following command:

```
RpsRpf.cmd
```

Linux

Run the following command:

```
./RpsRpf.sh
```

Note: If a framework generation process is already in progress, the script returns information about the process.

7. Check the log file for errors and warnings: `<client_tools>/logs/openpages-tools-client.log`

Where `<client_tools>` is the directory that you used in step [“1” on page 122](#).

Chapter 8. Managing reports

IBM OpenPages with Watson contains a set of reports that allows users with the correct permissions to quickly view and organize data contained within OpenPages.

The **Pages and Templates** screen is used to add and manage report pages and page templates. It is typically used by administrators and report authors.

For information about the permissions you need to manage reports, see [“Publishing permissions” on page 59.](#)

Supplied reports

OpenPages with Watson comes with a selection of predefined and supplied reports that allow you to quickly view important information about your project.

Note: The list of reports in this documentation is for a fresh installation of OpenPages with Watson. If you have additional reports tailored to your particular business needs or have upgraded from an earlier version of the application, the classification of the supplied reports may differ from the classification documented here.

OpenPages platform reports

The **OpenPages Platform Reports** folder in OpenPages contains subfolders for the report types that are available.

<i>Table 62. OpenPages platform reports and folders</i>	
Report or folder name	Description
Administrative Reports folder	Folder that contains predefined administrative reports such as a list of files that are checked out.
Audit Reports folder	Folder that contains predefined audit reports such as an audit summary.
Common Code folder	Folder that contains the Common Code report, which contains the JavaScript for CrossTrack links.
Drill-Through Reports	Folder that contains the drill-through reports, such as the Issue Detail report.
Issue Reports folder	Folder that contains predefined reports on issues such as the issues and associated action items for a chosen reporting period and business entity.
Questionnaire reports	Folder that contains predefined questionnaire reports such as a program summary.
All Documentation report	Detailed view of an organization's entity hierarchy, associated internal controls documentation, and counts of related issues, files, and links in the current reporting period. This is filtered by business entity. There are detailed subreports for each count.
Carbon X Light report	A style reference report that is used by the pre-defined reports.

Administrative Reports folder

OpenPages with Watson includes the following, predefined administrative reports:

Table 63. Administrative Reports folder	
Report Name	Description
Checked Out Files	<p>Listing of attached files in a checked out state in the current reporting period.</p> <p>You can sort by:</p> <ul style="list-style-type: none"> • Name of the file. • Full path of the folder where the file is stored. • User who has checked out the file. • Date the file was checked out.
Disassociated Objects	<p>Listing of objects that do not have associated parent objects in the current reporting period. You can filter for specific object types and can sort by:</p> <ul style="list-style-type: none"> • Name of object. • Full Path of the folder where the object is stored.
Object Size	
Schema Analysis Report	

Audit Reports folder

In addition to the reports listed in the following table, the Audit Reports folder contains the following subfolders:

- Configuration (see [Table 66 on page 128](#))
- Security (see [Table 67 on page 128](#))

Table 64. Audit Reports folder	
Report Name	Description
Audit Change	<p>Lists all object changes that fulfill the user's runtime filtering criteria. Users can filter the report on Business Entity, Start Time, End Time, specific object type, and status. For an explanation of audit events and the values in the Status and Item columns of the report, see "Description of Audit Change events and values" on page 126.</p>
Audit Summary	<p>Administrative summary of changes to documentation data, which is filtered by date and time range. You can also filter by Business Entity and object type and drill into a detailed Audit subreport.</p>
Drill-Through Reports	<p>Folder that contains drill-through reports, such as the Audit Trail Detail report.</p>

Description of Audit Change events and values

An audit event is a combination of an action and object aspect (that is, the object, a relationship, or attribute of the object) that was affected by the event. The Audit Change report identifies change events for any field value change.

Notice: This information also applies to the detail subreport from the Audit Summary report.

To understand the nature of each audit event, it is useful to understand how objects are created, associated, and shared.

In the hierarchy of objects in the system, a child object (such as a Control) might be associated to more than one parent object (such as a Risk). Conversely, any one parent object (such as a Risk) might have

several associations to different child objects (such as Controls). These associations or relationships are flagged as either *Primary* or *Non-Primary*.

Any one parent object (such as a Risk) might have multiple child objects (such as Controls). However, the system allows only one of the object parent-child relationships to be marked as "Primary". Primary associations are used to determine the path that the system should follow when you are executing a number of operations that require object hierarchy traversal.

In the OpenPages with Watson application, the following operations traverse the Primary Association path:

- SCOR rule execution
- Cascade Delete (including those requested by SCOR delete rules)

SCOR is part of the object reset feature. For more information, see ["Object resets" on page 460](#).

- Sign-offs, Locking, and Un-Locking
- Hierarchical copy and move

Audit Trail Reports are "parent object centric" when the report captures events that pertain to an object associations. For an object, all association-related events are defined as those where the object acts as a parent. Events where the object acts as a child are reported in context of the corresponding parent objects.

Table 65 on page 127 lists the various audit change values that are listed in the **Action** column of the Audit Change Report with a brief description of the value and the affected object aspect.

Table 65. Audit Change Report values		
If the Status column has this value...	And the Item column has this value...	Then it indicates that...
Added	Association	An object was associated as a child object in the hierarchy.
Added	Object	A new object was created in the repository.
Added	Version	A new version of the object was created in the repository.
Changed	<property name>	The value of an object's system or extended property was modified.
Removed	Object	The object was logically deleted from the repository.
Removed	Association	An object was removed as a child object.
Removed Primary	Association	The association has been changed to Non-Primary. This could happen if the user selects another object relationship to be the Primary parent-child association or the current Primary association was deleted.
Added Primary	Association	The association type is set to Primary. This first association is always set to Primary

Table 66. Audit Reports Configuration subfolder

Report Name	Description
Configuration Audit	Lists all configuration changes made to the OpenPages with Watson application during the chosen date range.

Table 67. Audit Reports Security subfolder

Report Name	Description
Administrator Permissions	Lists each administrator and their granted permissions for each Security Domain they administer.
Security Domain Role Assignments	Lists each Security Domain to which the selected roles are assigned.
Login Activity Summary	Lists all users who accessed the OpenPages with Watson system during the date range. Each user is listed with the last login time, when they last changed their password, and how many times they logged in.
Login Activity Log	Lists all user activity during the specified date range. Report users can filter on date range, operation (log in or log out), login status (Failed or Succeeded), and number of login attempts.
Roles by Security Domain	Lists each role that is assigned to the selected Security Domain.
Roles by User	Lists each user and group with their assigned role for the selected Security Domain.
User Role Assignments	Lists all the roles in the system with the assigned user or group for each Security Domain.

Issue Reports folder

The following table identifies the Issue reports available in the Issue Reports folder:

Table 68. Issue Reports

Report Name	Description
Issue List	Detailed listing of Issues and associated parent objects, which are filtered by reporting period and Business Entity. Note: This report shows a subset of the Issues present in the system. To appear in this report, Issues must be associated with objects that are accessible through direct relationships in the default namespace. For example, Issues that are associated with Controls that are indirectly associated with a Risk Assessment will not appear. Issues associated with Risks that are directly associated in a chain, from Business Entity to Process or Subprocess to Control Objective, appear.

Table 68. Issue Reports (continued)	
Report Name	Description
Issues and Action Items	<p>Lists Issues and associated Action Items for the chosen reporting period and Business Entity.</p> <p>Note: This report shows a subset of the Issues and Action Items present in the system. To appear in this report, Issues must be associated with objects that are accessible through direct relationships in the default namespace. For example, Issues associated with Controls that are indirectly associated with a Risk Assessment will not appear, while Issues associated with Risks that are directly associated in a chain, from Business Entity to Process or Sub-process to Control Objective, will appear.</p>

Running reports from a dashboard

You can run reports that have been configured to display in your dashboard.

Before you begin

Configure the dashboard to display reports. For more information, see [“Home page, dashboard, and tabs” on page 230](#) and [“Defining a dashboard for a profile” on page 231](#).

Procedure

1. From the Home Page, open a dashboard panel for reports. Additionally, up to three reports can be configured as tabs on the Home Page.
2. Find the report you want to run, and click it.
The report is displayed.

Adding reports to OpenPages

To run a report, the report must first have a corresponding report page published to the OpenPages server.

A report page does the following:

- Makes it possible for the report to be added to dashboard panels.
- Specifies the parameters for launching the report.
- Specifies the keys used for localizing the report name and description.

All Cognos report pages are based on the CommandCenter Report page template, and all Cognos Workspace report pages are based on the CommandCenter Dashboard Redirect page template. Additionally, all IBM Cognos Analytics dashboard and story pages are based on the Cognos Analytics Dashboard Redirect page template. These templates are located at the root of the Reporting folder on the OpenPages with Watson server.

You can use the following methods to add new reports to OpenPages:

- Method 1: You can manually create the required report page and publish the report. This method is typically used for editing report pages and troubleshooting publishing issues.

For more information, see [“Method 1: Manually add and edit pages to create and modify reports” on page 130](#).

- Method 2: You can automatically generate the required report page and application text keys after identifying a Cognos report for publication.

For more information, see [“Method 2: Automatically publishing Cognos reports” on page 138](#).

Note: The actions you can take depend on your application permissions. For more information, see “[Publishing permissions](#)” on page 59.

Method 1: Manually add and edit pages to create and modify reports

You can use the **Pages and Templates** screen to add new pages or edit existing pages to create and edit reports.

This method is typically used for editing report pages and troubleshooting publishing issues.

Administrators can use the **Pages and Templates** screen to copy, move, and delete folders, report pages, and page templates.

Note: For more information, see [“Publishing permissions” on page 59](#).

Understanding reports

Reports are generated by combining report pages and page templates that provide necessary information about the filtering and sorting of the report contents, as well as the displayed name and description of the report.

Reports (both Cognos and JSP) are represented in a folder by a page template which lists the parameters that the source file needs in order to create a report. A report page is an instance of a page template, and contains a set of values for the parameters specified in the page template.

In this manner, a single page template can be supplied with multiple sets of values for its parameters. This allows the IBM OpenPages with Watson application to create multiple reports based on the same layout and internal logic. Each report page represents a report as viewed in OpenPages with Watson.

Report pages and page templates reside on the OpenPages with Watson server.

Note:

- Cognos reports can be published by using the **Add Cognos report** button on the **Pages and Templates** screen. This method automatically generates a corresponding report page and application text keys for localizing the selected report. For details, see [“Method 2: Automatically publishing Cognos reports” on page 138](#).
- Reports that are placed under the Reporting/SOX folder structure on the application server are published to the US English locale. To publish to a different locale, choose the /SOX folder under the locale you want (for example, ja_JP/SOX for the Japanese locale).
- All Cognos report pages are based on the Cognos Report Redirect page template, which is located at the root of the Reporting folder on the IBM OpenPages server.

Locating report files

Report files, such as report pages, page templates, and JavaServer Pages (JSP) reports, are located in the IBM OpenPages with Watson repository on the OpenPages with Watson server.

The OpenPages repository handles the data storage and access capabilities for the OpenPages with Watson application. To create, modify, or delete OpenPages reports, you must have an OpenPages with Watson account with permission to modify reporting folders. If you are not sure whether you have access to this functionality, contact your OpenPages administrator for additional information.

Accessing report pages and page templates

You can access report pages and page templates for JSP reports.

About this task

From the **Pages and Templates** screen, navigate through a hierarchy of folders and files. Each folder represents a report grouping in the IBM OpenPages user interface. Each page file represents an OpenPages with Watson report.

The **New Folder**, **New Page**, and **New Page Template** options are displayed if a folder is selected with a check mark. The **Copy**, **Move**, and **Delete** options are displayed if multiple folders or one or more report pages or page templates are selected with a check mark.

Note: The actions you can take depend on your application permissions. For more information, see “[Publishing permissions](#)” on page 59.

Procedure

1. Click  > **System Configuration** > **Pages and Templates**.
2. Navigate through the folder structure.

Manually creating an instance of a report

To manually create an instance of a report, you create a report page based on a copy of an existing page template.

About this task

Note:

- Cognos reports can be published by using the **Add Cognos report** button on the **Pages and Templates** screen. This method automatically generates a corresponding report page and application text keys for localizing the selected report. For details, see “[Method 2: Automatically publishing Cognos reports](#)” on page 138.
- Reports that are placed under the Reporting/SOX folder structure on the application server are published to the US English locale. To publish to a different locale, choose the /SOX folder under the locale you want (for example, ja_JP/SOX for the Japanese locale).
- All Cognos report pages are based on the Cognos Report Redirect page template, which is located at the root of the Reporting folder on the IBM OpenPages server.

Identifying the page template

You can determine which existing report page you want to copy from or use as the basis of a new report page.

About this task

If you already know the page template that you want to use, skip to the next task. Otherwise, complete this task to determine which existing report page you want to copy from or use as the basis of the new report page.

Procedure

1. Click  > **System Configuration** > **Pages and Templates**.
2. Navigate through the folder structure to find the report that you want to copy or use and modify as the basis of a new report.
3. Click the name of the report page to open it.

4. In the **General** section, note the value in the **Template** field. You will need to either reference this template or make a copy of the referenced template.

Creating a report page

To create a new report, you create a new report page based on a copy of an existing page template.

Procedure

1. Click  > **System Configuration** > **Pages and Templates**.
2. Navigate through the folder structure to the folder where you want the report page to be created.

For example, a report page for a new Cognos report in the U.S. English locale would be placed in the **Reporting/SOX/OpenPages Platform Reports** folder.

Optionally, create a category folder for grouping the reports under the appropriate /SOX folder. For example, to create a new report grouping titled "My Custom Reports" on the Reporting menu for the U.S. English locale, you could create a folder with the path **Reporting/SOX/My Custom Reports**. Any report pages placed in the folder will appear under that grouping in a dashboard reports panel in OpenPages.

3. Select the folder with a check mark.
4. Click **New Page**.
5. Enter a **Name** for the report.

Note: You will not be able to change the name of a report after it is created.

6. In **Template**, choose the page template that you want to use to create the report.
 - For Cognos reports that you want to run from the Home Page, use the **CommandCenter Report Redirect** page template.
 - For Cognos reports that you want to run by clicking on a URL launcher field in a view, use the **CommandCenter Report Redirect for Cognos Reports** page template.

7. Enter a **Description** for the report.

8. Click **Save**.

The window expands to show more fields. The fields that are displayed vary depending on the template you choose. Click in each field to add a value or click **Edit Mode** to tab through the fields.

9. If this is a JSP report, skip to Step 11. Otherwise, for a Cognos report based on the **CommandCenter Report Redirect** or **CommandCenter Report Redirect for Cognos Reports** page template, do the following.

- a) Select a value for each of the following fields:

Table 69. Cognos report fields

Field Name	Description
Report Format	The display format for the report.
Show prompt page	Determines whether a prompt page is always displayed for a report. If the value is set to: <ul style="list-style-type: none">• Yes or true - a prompt page is always displayed even if the report has no required prompts.• No or false - a prompt page only displays if it is required by the report design. This value is set by default.
Report Folder	This field is optional. The report folders must be syntactically correct and separated by forward slashes. The Team content folder is assumed, and does not need to be included in the Report Folder field. For example, the report folder could be Vision 2019/Workspaces .

Table 69. Cognos report fields (continued)

Field Name	Description
Report Name	Type the report name that you want users to see in IBM Cognos Analytics.

- b) If you're using the CommandCenter Report Redirect template, complete the following additional fields:

Table 70. CommandCenter Report Redirect fields

Field Name	Description
Report Type	<p>The IBM Cognos Studio application used to develop the report. Valid values are:</p> <ul style="list-style-type: none"> • report (for IBM Cognos Analytics - Reporting, this is the default value) • query (for Cognos Query Studio) • analysis (for Cognos Analysis Studio) • pagelet (for Cognos Workspace, a type of dashboard that can contain multiple content pieces, including reports, on a single page)
Open with	<p>The method for opening the report. Valid values are:</p> <ul style="list-style-type: none"> • CognosViewer - opens the report in view-only mode, this is the default value. • ReportStudio - opens the report in IBM Cognos Analytics - Reporting so it can be modified. • QueryStudio - opens the report in Cognos Query Studio so it can be modified. • AnalysisStudio - opens the report in Cognos Analysis Studio so it can be modified. • CognosWorkspace - enables the report to be opened in Cognos Workspace.

- c) If you're using the CommandCenter Report Redirect for Cognos Report template, complete the following additional fields:

Table 71. CommandCenter Report Redirect for Cognos Report fields

Field Name	Description
resourceid	The ID of the object for the report.
reportingPeriodId	The reporting period to use for the report.

- d) Skip to Step 12.

10. For a report based on the CommandCenter Dashboard Redirect page template, do the following:

- a) Click the **Mode** arrow and select the method for opening the dashboard.

Valid values are:

- **view** (opens the dashboard in view-only mode, this is the default value)
- **edit** (opens the dashboard in Cognos Workspace so it can be modified)

- b) Skip to Step 12.

11. For a JSP report, enter the sorting and filtering information for the report.

12. Enter values for all required fields (required fields have a red asterisk *) including key field information as follows:

Table 72. Report Page Key Fields

Key Field	Format	Description
Report Name Key	report.name.<user-defined> Example report.name.control.analysis	A key that references an application text string for localizing the title of the report.
Report Description Key	report.description.<user-defined> Example report.description.control.analysis	A key that references an application text string for localizing a description of the report.

Note: You can use the values in the **Report Name Key** and **Report Description Key** fields on the report page to manually create custom application text keys to localize the name and description of a report after it is created. For details, see “[The Custom folder](#)” on page 455.

13. Click **Save**.

Results

When you log on to OpenPages, the new dashboard or story should be visible in dashboard reports panels.

What to do next

If you used the CommandCenter Report Redirect or CommandCenter Report Redirect for Cognos Report template and you want to pass in report parameters from OpenPages, see “[Configuring parameters for Cognos reports](#)” on page 134.

Configuring parameters for Cognos reports

If you want to pass values from IBM OpenPages with Watson to your Cognos report, you need to add the parameters to the report template in OpenPages.

About this task

For example, suppose you have a URL launcher field that opens a report. The URL configuration string includes a parameter that passes in the name of a project to the report. In this case, you need to add the project name parameter to the CommandCenter Report Redirect for Cognos Report template.

This task applies to report pages that are based on the CommandCenter Report Redirect for Cognos Report and CommandCenter Report Redirect templates. If you’re creating an interactive JSP report, see “[Creating an interactive JSP report](#)” on page 139 instead.

Procedure

1. Click  > **System Configuration** > **Pages and Templates**.
2. Click the template that your report is using: CommandCenter Report Redirect or CommandCenter Report Redirect for Cognos Report.
3. In the **Parameters** section, click **Add Parameter**.
4. Configure the parameter.
5. Set **Interactive Value** to **False**.
6. Click **Done**.

7. Repeat these steps for each parameter.
8. Click **Save**.
9. Go to each report that uses the parameter you added. Make any change to the report and save it.

Every time you make a change to the CommandCenter Report Redirect or CommandCenter Report Redirect for Cognos Report page template, you need to make a change to the consuming report in order for the change to work.

Modifying a report page

You can modify an existing report page.

Procedure

1. Click  > **System Configuration** > **Pages and Templates**.
2. Navigate through the folder structure to the folder that contains the report that you want to modify.
3. Click the report name.
4. Make your changes. Click in each field to change a value or click **Edit Mode** to tab through the fields.

Note: You cannot modify the name of a report. In order to change the name of a report, you must delete the misnamed report and create an identical report with the new name.

As an alternative, you can use the values in the Report Name Key and Report Description Key fields on the report page to manually create custom application text keys to localize the name and description of a report after it is created. For details, see “[The Custom folder](#)” on page 455.

5. Click **Save**.

The modified information is saved and immediately applied to the dashboard or story.

Deleting a report

Super administrators and members of the OPAdministrators group can delete reports.

About this task

You can delete an instance of a JSP report or report page for a Cognos report.

Procedure

1. Click  > **System Configuration** > **Pages and Templates**.
2. Navigate through the folder structure to the folder that contains the report that you want to delete.
3. Click **Delete**.
4. Click **OK** to delete the report page (or JSP report instance).

 **Attention:** Do not delete a page template. If a page template is deleted, all report pages based on that template are deleted as well.

Manually creating an instance of a Cognos dashboard or story

To manually create an instance of a Cognos dashboard or story, you create a dashboard or story page based on a copy of an existing page template.

- Dashboards and stories that are placed under the Reporting/SOX folder structure on the application server are published to the U.S. English locale. To publish to a different locale, choose the /SOX folder under the locale you want (for example, ja_JP/SOX for the Japanese locale).
- All Cognos dashboard and story pages are based on the Cognos Analytics Dashboard Redirect page template, which is located at the root of the Reporting folder.

Note: The actions you can take depend on your application permissions. For more information, see “[Publishing permissions](#)” on page 59.

Identifying the dashboard or story page template

You can determine which existing dashboard or story page you want to copy from or use as the basis of a new dashboard or story page.

Procedure

1. Click  > **System Configuration** > **Pages and Templates**.
2. Navigate through the folder structure to find the dashboard or story you want to copy or use and modify as the basis of a new dashboard or story.
3. Click the name of the dashboard or story page.
4. In the **General Information** section, note the value of the **Template** field. You will need to either reference this template or make a copy of the referenced template.

Creating a dashboard or story page

To create a new dashboard or story, you create a new dashboard or story page based on a copy of an existing page template.

Procedure

1. Click  > **System Configuration** > **Pages and Templates**.
2. Navigate through the folder structure to the folder where you want the dashboard or story to be created.

For example, a dashboard page for a new Cognos dashboard in the U.S. English locale would be placed in the **Reporting/SOX/OpenPages Platform Reports** folder.

Optionally, create a category folder for grouping the dashboards or stories under the appropriate /SOX folder. For example, to create a new dashboard grouping titled "My Custom Cognos Dashboards" on the Reporting menu in the OpenPages with Watson application for the U.S. English locale, you could create a folder with the path **Reporting/SOX/My Custom Cognos Dashboards**. Any dashboard pages placed in the folder will appear under that grouping in the reporting sections of the OpenPages with Watson application.

3. Select the folder with a check mark.
4. Click **New Page**.
5. Enter a **Name** for the dashboard or story.

Note: You will not be able to change the name of a dashboard or story after it is created.

6. In **Template**, choose the page template you will use to create the dashboard or story.
Cognos dashboards and stories use the **Cognos Analytics Dashboard Redirect** page template.
7. Click **Save**.
The window expands to show more fields. Click in each field to add a value or click **Edit Mode** to tab through the fields.
8. Select a value for each of the following fields:

Table 73. Cognos Analytics Dashboard Redirect Selection Fields

Field Name	Description
Action	Select the method for opening the dashboard or story. Valid values are: <ul style="list-style-type: none">• view (opens the dashboard or story in view-only mode, this is the default value)• edit (opens the dashboard or story in Cognos Workspace so it can be modified)
Mode	Select the page mode. Valid values are: <ul style="list-style-type: none">• dashboard• story
Dashboard (or) Story Folder	The dashboard or story folders must be syntactically correct and separated by forward slashes. The Team content folder is assumed, and does not need to be included in the Dashboard (or) Story Folder field.
Dashboard (or) Story Name	The dashboard or story name must be the name that you want to appear in IBM Cognos Analytics.

9. Click **Save**.

Modifying a dashboard or story template

You can modify an existing dashboard or story template.

Important: If you want to modify the supplied dashboard and story template for your own purposes, you must copy it to a new location outside the SOX folder structure, and then modify the copied template. Otherwise, you will risk losing your changes when upgrading to a newer version of the IBM OpenPages with Watson application.

Procedure

1. Click  > **System Configuration** > **Pages and Templates**.
2. Navigate through the folder structure to the folder that contains the dashboard or story that you want to modify.
3. Click the dashboard or story name.
4. Make your changes. Click in each field to change a value or click **Edit Mode** to tab through the fields.

Note: You cannot modify the name of a dashboard or story. To change the name of a dashboard or story, you must delete the misnamed report and create an identical report with the new name.

As an alternative, you can use the values in the Report Name Key and Report Description Key fields on the report page to manually create custom application text keys to localize the name and description of a report after it is created. For details, see “[The Custom folder](#)” on page 455.

5. Click **Save**. The modified information is saved and immediately applied to the report.

Deleting a dashboard or story

You can delete an instance of a dashboard or story page for a Cognos dashboard or story.

Procedure

1. Click  > **System Configuration** > **Pages and Templates**.

2. Navigate through the folder structure to the folder that contains the dashboard or story that you want to delete.



Attention: Do not delete a page template. If a page template is deleted, all dashboard or story pages based on that template are deleted as well.

3. Click **Delete**.

4. Click **OK**.

Method 2: Automatically publishing Cognos reports

You can automatically publish Cognos reports by using the **Add Cognos report** button on the **Pages and Templates** screen.

When you add a Cognos report by clicking the **Add Cognos report** button on the **Pages and Templates** screen, the following process occurs:

- A corresponding report page is automatically generated on the OpenPages with Watson server that is based on the **CommandCenter Report Redirect** page template.
- The report is published, by default, to the U.S. English locale.
- If the report name and description are not specified for a locale, the values in the U.S. English locale are used by default.
- Report name and description application text keys are automatically created in the "Miscellaneous" folder on the **Application Text** page and populated with the specified values.

These key values are used for localizing the report name on any dashboard panels that include all reports. To modify these key values, see ["Localizing application text" on page 447](#).

Before you begin

Before you can add a Cognos report, you must have details about the report available.

- The name of the report. Do not enter special characters, including the underscore, in the report name.
- A description of the report
- The path and name of the folder to be deployed (the folder selection is filtered to list report folders only). By default, the path is `/_cw_channels/Reporting/SOX`.

Example

A new unpublished report was created called "My Control Summary" in the `OPENPAGES_SHARED` folder on the Cognos server. Publish the report to make it available for users in the US English and Japanese locales.

On the **Pages and Templates** screen, click the **Add Cognos report** button. Click **Choose** next to **Select Cognos report** and select the report from the listing. For the US English locale (this locale is automatically selected by default), type in "My Control Summary" for the report name, and "All controls assigned to me" as the description for the report. You then select Japanese in the **Additional languages**, add a report name and description or click **Auto Translate** (if Watson Language Translator is enabled), and select the folder for the report.

The application text keys for the "My Control Summary" report that are automatically generated under the "Miscellaneous" folder on the Application Text page may look similar to these: `report.name.openpages.shared.my.control.summary` and `report.description.openpages.shared.my.control.summary`.

You can use these keys to modify the report name or description that is displayed on the application user interface for a locale.

Attention: To view the new report on the Reports menu, users must log out and log back in to the application.

Report publishing limitations

Publishing report pages by using the **Add Cognos report** button has some limitations.

- You can publish only one report at a time.
- If you want to edit existing reports, you must be a member of the OPAdministrators group to edit the report page. For more information, see “[Modifying a report page](#)” on page 135.
- If the initial publishing process failed to publish a report to any locale other than English, you must create a new page to add the report. For more information, see “[Manually creating an instance of a report](#)” on page 131.

Publishing a report

The Report selection list in the **Add Cognos report** panel contains all available reports that are not already published.

Procedure

1. Click  > **System Configuration** > **Pages and Templates**.
 2. Click **Add Cognos report**.
 3. Select a report from the Report list.
 4. In the **Name** field for each selected locale, type the display name of the report.
This name will be displayed to users on reports panels on user dashboards.
 5. In the **Description** field for each locale, type a description of the report.
- Note:** Any locale for which you do not specify a localized name and description will, by default, contain the U.S. English name and description.
6. Click **Choose** next to **OpenPages folder** and select a folder where the report will be located.
 7. To publish the report in another locale, select a language in the **Additional languages**. Add a name and description for each selected locale, or use the Auto Translate feature if Watson Language Translator is enabled. For each locale, select the folder where the report will be located.
 8. Click **Add**.

After the report is published, a link to launch the report is displayed on the Reports page along with a description of the report, and the report name is added to the list of selections on the Reporting menu.

Modifying the displayed report name or description

You can localize and modify the name and description that is displayed to users on the IBM OpenPages with Watson for a report in a given locale.

You do this by locating the application text keys that correspond to the name and description of the report and then modifying the value in the key for that locale.

For more information and instructions, see “[Modifying application text](#)” on page 449.

Creating an interactive JSP report

The IBM OpenPages with Watson application allows administrative-level users with the option to create interactive reports to prompt a user at run-time for parameter values. You can either modify an existing JSP report to be interactive, or specify an interactive parameter during report creation.

Procedure

1. Click  > **System Configuration** > **Pages and Templates**.
2. Navigate through the folder structure to find the page template for the report that you want to modify.
3. Click the name of the page template you want to modify.

4. Scroll down to the **Parameters** section.
5. Click the name of the parameter that you want to make interactive.
The parameter information is displayed.
6. Set **Interactive Value** to **true** and click **Done**.
7. Repeat the steps for each parameter that you want to make interactive.
8. Click **Save**.
9. Go to each report that uses the parameter that you added. Make any change to the report and save it.
Every time you make a change to a page template, you need to make a change to the consuming report in order for the change to work.

Results

The next time the report is run, the user will be prompted to enter a value for each field marked as an interactive value.

Important: Reports with an interactive parameter named "label" are a special case and will not display a dialog to enter a value for "label". The "label" field is included to support reporting periods and should not be modified.

Note: Although any parameter type can be defined as an interactive parameter that requires a user to provide information at run time, IBM OpenPages supports only the following four modes of entering values into the value fields when the report is run:

- Date fields
- Text entry fields
- Enumerated drop-downs
- File browsers

Unsupported types might be marked as interactive. However, the value for these fields must be entered manually, using a text string at run time. A valid value must be entered into the value field for the report to return the correct set of information.

What to do next

For information about running an interactive report, see ["Running an interactive JSP report" on page 140](#).

Running an interactive JSP report

The IBM OpenPages with Watson application allows administrative-level users with the option to create interactive reports to prompt a user at run-time for parameter values.

Note: Although any parameter type can be defined as an interactive parameter that requires a user to provide information at run time, IBM OpenPages supports only the following four modes of entering values into the value fields when the report is run:

- Date fields
- Text entry fields
- Enumerated drop-downs
- File browsers

Unsupported types might be marked as interactive. However, the value for these fields must be entered manually, using a text string at run time. A valid value must be entered into the value field for the report to return the correct set of information.

Procedure

1. From the Home Page, open a dashboard panel for reports.

2. Find the report you want to run, and click it. If the report contains interact parameters, a prompt page or panel is displayed.
3. Enter information in the required fields.
When you are finished, the report is displayed.

Restricting access to reports

To restrict access and set security on reports, you need to set permissions in OpenPages and in IBM Cognos Analytics.

Note: If you restrict access to reports only through IBM Cognos Analytics, but not in OpenPages, the reports might be displayed in a selection list to users in a report dashboard panel. If a group or user who does not have permission selects the restricted report, the report will not run and an error message is displayed to the user.

Setting permissions on JSPs and reports

You can restrict users and or groups from accessing and running JSP reports from OpenPages by setting Read, Write, Delete, and Manage permissions on selected report folders.

About this task

For example, if you want only administrators in a System Administrators group to have access to administrative reports, you could set Read, Write, Delete, and Manage access on the Administrative Reports subfolder (which is under the **SOX > Cognos** folder). After you grant access to administrative reports for the System Administrators group, you can then break inheritance on the folder to restrict other users and groups from accessing these reports.

Procedure

1. Click  > **System Configuration > Pages and Templates**.
2. Navigate through the folder structure. Expand the folders, if necessary.

Note:

- Each folder represents a report grouping in OpenPages.
 - Reports that are under the Reporting/SOX folder structure are published to the U.S. English locale. To select a different locale, choose the /SOX folder under the locale you want (for example, ja_JP/SOX for the Japanese locale).
3. Click the name of the folder that contains the reports to which you want to limit access.
The folder properties are displayed.
 4. Scroll down to the **Access Control** section.
 5. Click **Add Access Control**.
 - a) Select a group or user to whom you want to grant permission.
 - b) Select the permissions you want to allow or deny the group or user (Read, Write, Delete, Manage).
 - c) Click **Add**. The selected group or user appears in the list.
 - d) To select another group or user, repeat steps a-c.
 - e) To remove a group or user, select the group or user then select **Remove**.
 6. Break inheritance on the folder so that other groups or users cannot access these reports from OpenPages:
 - a) In the properties for the folder, set **Inherit ACL** to false.
 7. Click **Save**.

Securing access to the report portal

You can restrict which user groups are allowed to modify reports.

Note: This task is optional.

Use the following tasks to allow a group, in this example the OPAdministrators group, to update, add, and delete reports, and to restrict other users from changing settings within IBM Cognos Analytics:

- [“Assigning CommandCenter administrative rights to a group” on page 142](#)
- [“Specifying user access to administrative functions in IBM Cognos Analytics” on page 142](#)
- [“Restricting access to reports in the Team content folder” on page 143](#)
- [“Restricting users to only running reports” on page 144](#)

Note: IBM OpenPages with Watson standard reports might be overwritten during an upgrade. If you want to modify the standard reports, copy the reports to your own folder structure where you can then modify and control access to these reports.

Assigning CommandCenter administrative rights to a group

Before you can specify access rights and restrictions to reports and reporting functions, you must assign CommandCenter administrative rights to a new or existing group.

Procedure

1. Log on as a user with administrative privileges.
2. Create a group in to which you want to give CommandCenter administrative rights, or use an existing group, such as OPAdministrators.

Note: For information on creating groups, see [“Creating an organizational group” on page 51](#).

Specifying user access to administrative functions in IBM Cognos Analytics

You can specify which users have access to administrative functions within the IBM Cognos Analytics.

Procedure

1. From a browser, log on to IBM Cognos Analytics as a user with administrative privileges, for example, OpenPagesAdministrator.

By default, the URL is:
`http://<hostname>/ibmcognos/bi` (if you are using port 80 for Cognos)

Where <hostname> is the name of the Cognos server.
2. Click **Manage > Administration Console** to launch the **IBM Cognos Administration** page.
3. On the **Security** tab, click the **Cognos** link in the **Directory** list.
4. On the **Directory > Cognos** page:
 - a) Locate the System Administrators group in the list.
 - b) Click the **More** link in the same row as the System Administrators group.
5. Under **Available Actions** on the **Perform an Action** page, click the **Set members** link.
6. On the **Members** tab of the **Set Properties** page, click the **Add** link.
7. On the **Select entries (Navigate)** page, do the following:
 - a) Click the **OpenPagesSecurityRealm** link to find the IBM OpenPages with Watson group or role to access CommandCenter administrative functions.
 - b) Select a group. For example, OPAdministrators.
 - c) Click the green arrow to add the role.

8. On the **Members** tab of the **Set Properties** page, restrict access to the administrative functions.

- Select the Everyone group.
- Click the **Remove** link.

Restricting access to reports in the Team content folder

You can restrict users' access to reports that are in the **Team content** folder in IBM Cognos Analytics.

Procedure

- On the IBM Cognos Analytics page, click the **Team content** folder.
- On the **Team content** page, click the **List view** icon.
- Select a folder, and then click **Properties**.
- Click the **Permissions** tab and do the following:
 - If not already selected, select **Override parent permissions**.
 - Click the **Add** icon.
- In the **Select entries (Navigate)** window, click the **Cognos** link, and do the following:
 - Select the group to be added (for example, System Administrators).
 - Click **Add**, and then click **Close**.
- On the **Permissions** tab, do the following:
 - In the **Permissions** column for the group that you added, click the permission. For example, click **Read**. Do not use the drop down menu.

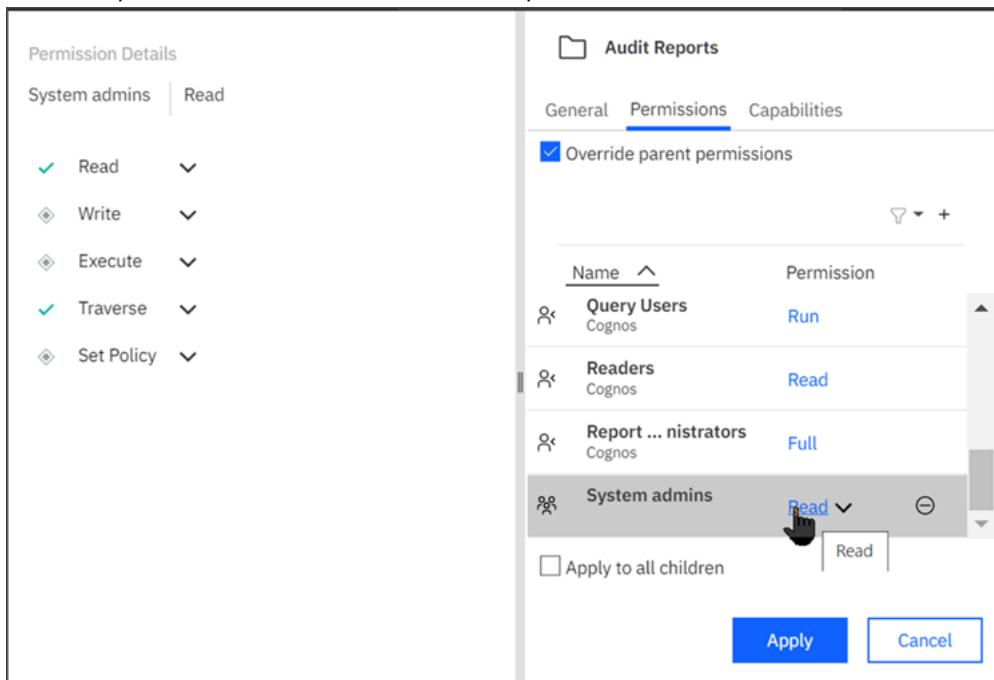


Figure 11. Assigning permissions in Cognos

- Grant the group Read, Write, Set Policy, and Traverse permissions.
- Remove the Write and Set Policy permissions from the other groups.

Now, if a user logs on to IBM Cognos Analytics with a user name that is not in, for example, the System Admins group, and the user tries to delete, change, or save a report in the folder, an error message is displayed to the user.

For information about how to set permissions for features and functions, see [Setting access to capabilities](#) in the Cognos documentation.

Restricting users to only running reports

You can restrict users to only run reports, with no access to IBM Cognos Analytics to modify reports.

About this task

Use the features in IBM Cognos Analytics to manage user access. For more information, see [Authorization](#) in the IBM Cognos Analytics documentation

The users and groups that are configured in OpenPages are available in IBM Cognos Analytics in the **OpenPagesSecurityRealm** namespace.

Chapter 9. System file management

The ability to manage system folders and files is essential for information management in IBM OpenPages with Watson.

Using the **System Files** area of OpenPages you can complete the following tasks:

- View folders and files
- Manage folders and files
- Search for files

Object types

The **System Files** area of OpenPages contains five types of system files (content file types). Four types are unique system file types, but the fifth type, Files (SOXDocument), can be either system files or non-system files.

The content file types are defined as the following object types in OpenPages:

- Files (SOXDocument)
- SysXMLDocument
- ExporterXML
- MigrationJAR
- Report

You manage these object types like other object types in the system.

<i>Table 74. Object types for files</i>	
Object type	Description and examples
Files (SOXDocument)	System and non-system files <ul style="list-style-type: none">• DefaultTemplate.xlsx (example of a system file)• attachments that users add to objects (examples of non-system files)

Table 74. Object types for files (continued)

Object type	Description and examples
SysXMLDocument	<p>End user application configuration JSON and trigger configuration files</p> <ul style="list-style-type: none"> • The root storage folder contains the _trigger_config.xml file. • The TriggerConfigFiles folder contains trigger configuration files, such as:openpages-solutions.xml, OPLC-Incident.xml, and so on. <p>The trigger configuration files must also be listed in the Applications > GRCM > Trigger Configuration Files setting. For more information, see the <i>IBM OpenPages with Watson Trigger Developer Guide</i>.</p> <ul style="list-style-type: none"> • The End User Applications Config folder contains end user application configuration files such as: <ul style="list-style-type: none"> – IBM OpenPages Loss Event Entry: lossevent_config.json – Natural Language Classifiers: the classifiers folder contains JSON files. Each file contains connection information for an instance of a Natural Language Classifier. For more information, see “Defining a classifier configuration” on page 854. • The Taxonomy folder contains taxonomy files, which are used by IBM OpenPages Regulatory Compliance Management.
ExporterXML	<p>Notification reports</p> <p>Expand the _exporter folder to see the files.</p>
MigrationJAR	<p>JAR files that are imported by using  > System Migration > Import Configuration and exported by using  > System Migration > Export Configuration</p> <p>Expand the Migration Documents folder to see the files.</p> <p>Example: openpages-env-mig_<timestamp>.jar</p>
Reports	<p>JSP files, for example, solution helpers, Command Center redirects, FastMap reports, and more</p> <p>Expand the Reports folder to see the report files.</p> <p>Example: Reports/SOX/ORM Custom Reports/ORM_IMRBulletin.jsp</p>

Access permissions for folders and files

Not all folders and files are accessible to all users. Each folder and file can have its own set of access permissions that determine which users are allowed to view or edit it. Sensitive or private information remains visible only to selected users, most often to prevent accidental editing or deletion.

Each user can view only the folders and files to which they have access permissions. Each user's view of the file system can appear differently, although all users are typically working from the same set of data. For example, one user can have access to all folders and files and be able to see all files in the system. Another user can have access to only a limited set of folders and files, which makes the folders and files to which they do not have access uneditable.

Note: The creator of a file is automatically granted all access permissions to that file, regardless of the limitations set by a group or the folder where the file is located.

Access to the System Files menu item

The OpenPages Platform 3 profile includes access to all of the system file types. An administrator assigned this profile has access to all the system files and folders.

Add the ready-to-use OpenPages Platform 3 profile to the list of available profiles for your administrators who manage system files. Using this profile, you have access to the  > **System Configuration > System Files** menu items.

If you do not use the OpenPages Platform 3 profile, you can add the system file object types to any other profiles that administrators use. Users must be members of the OPAdministrators user group for the  > **System Configuration > System Files** menu item to display.

Version control in the file repository

OpenPages uses version control and file locking in the file repository. When you work in a collaborative team environment, files are checked in and out to ensure that changes made by one team member will not be overwritten by another team member.

When you add a file, a copy of the file is uploaded to the OpenPages file repository. After a file has been added:

- Click the file name to view file details and access multiple versions of the file if they exist.
- Click  to download it.

Click **Check Out** to check out a file.

A checked-out file has the following characteristics:

- A checkmark is displayed next to the file name. If it is green, you checked it out. If it is blue, it is checked out by another user.
- The file is locked and cannot be overwritten in the file repository.
- The last checked in version and all earlier versions of the file can be viewed and downloaded by other users.

When you check in a file, you can add a comment. A new version is then uploaded with your latest changes, the file is unlocked, and it is available to other users to view and check out.

Accessing files and folders

System files and folders are accessed with the  > **System Configuration > System Files** task.

Non-system files are accessed with the **Attachments > Files** task. Users can also add non-system files directly to objects from Task Views.

Table 75. Where to access files	
To access this type of file ...	Go to ...
Files (SOXDocument)	 > System Configuration > System Files (system files) or Attachments > Files (non-system files)
SysXMLDocument	 > System Configuration > System Files and then expand the End User Applications Config folder or Trigger Config Files folder
ExporterXML	 > System Configuration > System Files and then expand the _exporter folder

Table 75. Where to access files (continued)

To access this type of file ...	Go to ...
MigrationJAR	 > System Configuration > System Files and then expand the Migration Documents folder
Reports	 > System Configuration > System Files and then Expand the Reports folder

Managing system files and folders

To enable you to manage your content effectively, changes often need to be made to your folder and file structure, including changing file locations, changing file and folder names, and removing unwanted content from IBM OpenPages with Watson.



CAUTION: System files must have specific names and be in specific folders so use caution when moving, deleting, or renaming these types of files or their folders.

Use the  > **System Configuration** > **System Files** task to manage system files and folders.

You need to be a member of the OPAdministrators group to use the  > **System Configuration** > **System Files** menu item.

Working with files

From the list of system files and folders, you can work with files:

- Click  to search for files by object type.
- Expand and collapse folders to navigate to the file you want to work with.
- Select the check box next to a single file. The bulk update options are:
 - **Rename**
You can rename a folder or file only if you have the correct permissions to do so.
 - **Copy**
 - **Move**
 - **Delete**
- Select the check box next to multiple files to update numerous files. The bulk update options are:
 - **Copy**
 - **Move**
 - **Delete**
- Add, download, and modify system files. For more information, see [“Adding and modifying system files” on page 150](#)

Working with folders

From the list, you can work with folders:

- Click a folder name. The folder details and access controls are displayed.
- Select the check box next to a single folder. The bulk update options are:
 - **New** (to add a new file to the folder)
 - **New Folder** (to add a new folder)

You can create a new folder within any folder for which you have access permissions.

- **Copy**
- **Move**
- **Delete**
- **Rename**
- Select the check box next to multiple folders to update numerous folders. The bulk update options are:
 - **Copy**

Moving files and folders

If you attempt to move a file into a folder that already contains a file with the same name, the file will not be moved. If you paste the file into a folder that does not already contain a file with the same name, then the original file name will be used.



CAUTION: Because some files are referenced by other system processes, and because other users may be working with common files, ensure that you are not going to inadvertently disrupt the work or files of others before moving a file.

Deleting files and folders

When you delete a folder, the folder and all of its contents are removed from IBM OpenPages with Watson. When you delete a file, it is removed from OpenPages. You can only delete a folder or file if you have the appropriate access permissions.



CAUTION: Because some folders and files are referenced by other system processes, and because other users may be working with shared files, please ensure that you are not going to inadvertently disrupt the work of others before deleting content.

Assigning access control to folders

You can control which users and groups can access files. Access controls (ACL) are defined at the folder level and apply to all files within the folder. They are defined by users and groups.

Click , and then click **New Access Control**. Select a user or group. For each permission (Read, Write, Delete, Manage), select a setting value (Granted, Inherited, or Denied).

Opening files and folders in a Quick View

Click to open a file or folder in a Quick View. The file or folder opens in the side panel.

Click to open the file or folder in its own tab. Full functionality is then available.

System file modification

You can download a copy of a file to view if you have view permissions for the file or you can edit a file by checking it out of IBM OpenPages with Watson.

When you check in an updated file, the original file is updated in OpenPages with the newer edited version. If file versioning is enabled, then older versions of files are maintained as you make edits. The most recently checked in version of a file is considered as the current version.

Adding and modifying system files

Use the  > **System Configuration** > **System Files** task to add and modify system files.

About this task

Only super administrators and members of the OPAdministrators group can create or modify system JSP files in the /Report folder.

For more information about system files and folders, see [“Managing system files and folders ” on page 148.](#)

Procedure

1. Click  > **System Configuration** > **System Files**.

2. To add files to a folder:

- a) Navigate to the folder where the file will be saved.
- b) Select the check box next to a folder and click **New**.
- c) Select an object type:

- File (SOXDocument)
- SysXMLDocument
- ExporterXML
- MigrationJAR
- Report

d) Enter a **Description**.

Fields and button labels vary depending on the object type you chose. They may also vary depending on how your system is configured.

e) Click **Add File** and select the file. Only file types that match the object type are available to be selected.

f) If you chose **File** for the object type, click **Select Folder** and associate the file to a parent object. You might also be able to add keywords and select a document type.

g) Click **Save**.

The file is added and automatically checked in.

After a file has been added, there are two methods to upload a new version of it. Using either method, you receive an error message when you upload the file if it is checked out by another user.

3. To update a file using manual check out:

Use this method to prevent other users from editing the file while you are working on your changes.

- a) Click a file.
- b) Click **Check Out**. The icon is hidden if the file is already checked out.
- c) Download the file.
- d) Make and save your changes to the file.
- e) Click **Update** and select the file. Alternatively, you can drag the file to the page.
- f) Complete the fields in the **Files to update** pop-up window.
- g) Click **Upload**. Your copy is uploaded and checked in.

You can click **Cancel Check Out** to cancel a check out. If you cancel a check out, OpenPages reverts to the last checked in version of a file in the file repository.

4. To update a file without using manual check out:

Use this method if you are making quick changes to the file.

- a) Click a file.
- b) Download the file.
- c) Make and save your changes to the file.
- d) Click **Update** and select the file. Alternatively, you can drag the file to the page.
- e) Complete the fields in the **Files to update** pop-up window.
- f) Click **Upload**. The file is automatically checked out and back in.

Refreshing trigger configurations

In IBM OpenPages with Watson, you can use the Trigger Configuration Refresh Utility to apply new or updated trigger XML configuration files as well as changes to the triggers registry settings.

About this task

By default, only users in the OPAdministrators group and super administrators have access to this utility. Running this utility refreshes the trigger cache. Updates to JAR files are not refreshed by this utility. The application server must be restarted for new JAR files to be loaded.

Procedure

1. Click  > **System Configuration** > **Pages and Templates**.
2. Go to **Reporting** > **SOX** > **OpenPages Platform Reports** > **Configuration Utilities**.
3. Select **Trigger Configuration Refresh Utility**.

Chapter 10. Fields and field groups

A field group is a container for fields that store information in OpenPages.

Definition of fields

An object field represents information that is stored in OpenPages.

Object fields are defined and managed by using > **Solution Configuration > Object Types**. Aspects of their assignment to profiles are managed by using > **Solution Configuration > Profiles**.

To define an object field:

- Add the field to a new or existing field group.
- Associate it with a profile.

By default, each object type has a predefined field group that contains fields that are specific for that object type. For example, the "Effectiveness Rating" and "Operating Effectiveness" fields belong to the Control object field group called OPSS-Control.

丈, 工, 互, 乙, 且, 工,
鵠, 脣, 篤, 錄, 鑑

Important: Do not use the four-byte characters that are defined in the CJK Unified Ideographs EXTENSION-B Unicode Block Name in field values. These characters will not be saved.

Definition of a field group

Field groups are containers that organize fields into logical groups. They also allow you to more easily manage and share common fields across multiple object types. A field group can be assigned to multiple object types.

Fields and field groups are defined and managed by using > **Solution Configuration > Object Types**.

When a field group is associated with an object type, it is considered to be in use. When a field group is in use, you cannot delete the field group or any fields from that field group. You also cannot exclude the field group from an object type.

For example, you create a new field group that is called Extra Fields with three object fields, called Field 1, Field 2 and Field 3. You then add the new field group to the Risk object type. Even if you never display any of the new fields on any Risk object view page, the Extra Fields field group is in use and cannot be deleted.

Note: If a management operation is being modified by two administrators at the same time, an error message is displayed, notifying you to try again later.

Requirements for new fields

Before you create a new field, determine the characteristics of the field and the object types that will use the new field.

The following list identifies information that is needed before you create a new field:

- Object - Identify the object types where the new field will be added. Decide which object to use first. You can add the field to other object types later.
- Field group - Should the field be added to an existing field group or do you need a new field group? Consider categorizing collections of field definitions in the same field group for ease of maintenance.

- Name - How will the new field be identified? The name is important because it is also the default label that appears next to the field. Special characters cannot be used. For more information, see “[Field naming guidelines](#)” on page 154.
- Label - What text do you want to display next to the field when this field appears in a view? Add a label to give the field a more meaningful name for users. You can also add labels for different locales. When a user opens a view that contains the field, for example, the translated label is what they see. For more information, see [Chapter 18, “Localizing text,” on page 443](#). If you don’t add a label, the field name is displayed.
- Data type - What is the type of data, such as Boolean or Date, that is captured by the field? For some data types, for example, Simple String, you can also specify a Display Type. The display type determines how the field is presented to the user. For more information, see “[Data types](#)” on page 155.
- Required? - Is the user required to enter data in this field or is data entry optional? Is data entry always required or is it required only in certain contexts? When a field is set to Required, the setting applies to the field no matter where it is displayed. If you want the field to be required only in certain contexts, set the field to Required in the view definition or within field dependencies instead. For more information, see “[Making fields required or optional](#)” on page 162.
- Global search - If you use global search, do you want this field to be indexed and used for global search?
- Encrypted - If the field is defined as a simple string or long string data type, decide whether the field values should be further secured by using encryption. For more information, see “[Encrypting field values](#)” on page 163.
- Default value - Depending on the data type of the field, you can specify a default value. Do you want to set a default value for the field or do you want it blank? The default value is used when a new object instance is created. If you change the default value for a field, existing object instances are not updated.

Example

Suppose you want to add an Owner field to several object types. You can either create an **Owner** field and add it to the field group for each object type, or you can create a generic **Owner** field and field group for all object types and reuse it later if you want to add it to other object types.

To simplify the work, follow the generic approach and create a generic field group and field that can be added to any object type.

Plan the design of the new field:

- The new field needs a field group and a generic name. Name the field group **Custom Fields** and name the field **Owner**. The field label is important because it is the text that appears next to the field in the application, for example in views. You can provide different labels for different locales. For more information, see [Chapter 18, “Localizing text,” on page 443](#).
- The **Owner** field will be used to capture a name, so the data type for this field will be **User/Group**.
- Suppose you want objects to have only one owner. In this case, the display type for the field will be **User Selector**.
- Since the **Owner** field is considered important, make it a required field so that users must enter a name into the field before they can save and exit the page.
- The **User/Group** data type doesn’t support a default value. The initial value of the field will be blank.
- There are no other fields to be added to the **Custom Fields** field group. The **Owner** field is the only one you need for this example.

Now that you’ve planned the design, you’re ready to create the new field and add it object types.

Field naming guidelines

To create an object field that you can use in reports, you need to consider several factors when you name the field.

Do not use the object name in the field definition

IBM OpenPages with Watson uses a three- or four-character prefix convention when it generates the names for the Cognos framework model. When Cognos reports run, the prefix is converted to the object name in the column headers.

For example, in the supplied field definitions, the **OPSS-TestResult** field group contains a field that is named **Test Result**.

Table 76. Prefix conventions		
Prefix	Object type	Report column header
RI_	SOXRisk	Risk
CN_	SOXControl	Control
TR_	SOXTestResult	Test Result

When the Cognos framework model is generated, the **Test Result** field is converted to the query item **TR_TEST_RESULT**.

When the Cognos report is run, the **TR_TEST_RESULT** field column header displays as **Test Result Test Result** by default.

Criteria for naming fields

Ensure that you name fields by using the following criteria:

- Names must begin with the characters a - z or A - Z only. Names cannot begin with other characters such as numbers, spaces, hyphens, or underscores.
- Names can contain only the characters a - z, A - Z, 1 - 9, spaces, hyphens (-), and underscores (_).
- Limit the name definition to 20 character or less because names that exceed 20 are truncated.
- The framework generator reserves character positions 21 and 22 for a unique ID in the query item name. Field names that exceed 20 characters are truncated after the 20th character.
- The object prefix is not counted in these 20 characters.

If you have multiple field names that are more than 20 characters and have no unique characters in the first 20 characters, re-create the Reporting Schema only when necessary. The Cognos Reporting Schema generator might not generate the same two-digit unique ID for the field definitions for each reporting cycle. Reports that use these field definitions might not clearly identify each field definition.

Table 77. Example of names generated by the framework generator		
Reporting Schema generation	Field definition name	Name
Generation #1	Total Actual Financial Loss 2018	LE_TOTAL_ACTUAL_FINANCI01
Generation #2	Total Actual Financial Loss 2017	LE_TOTAL_ACTUAL_FINANCI01
Generation #3	Total Actual Financial Loss 2016	LE_TOTAL_ACTUAL_FINANCI01

If a long field name is required, create the name with unique characters at the beginning of the name. For example, instead of using the name **Total Actual Financial Loss 2022**, use the name **2022 Total Actual Financial Loss**.

Data types

The IBM OpenPages with Watson application provides various data types from which you can choose.

After you select a data type for a field and save it, only the parameters or settings for the data type can be modified; you cannot change the data type itself.

Boolean data type

A logical operator that has the following predefined values: **true** (default) or **false**.

For more information, see [“Defining Boolean fields” on page 164](#).

Business entity selector data type

A business entity selector data type field displays a business entity structure and allows users to move up and down the structure to locate and select a specific business entity. .

For more information, see [“Defining business entity selector fields” on page 165](#).

Classifier data type

The classifier data type accepts simple string text that can be interpreted and classified by a natural language processing service that uses Watson technology.

For more information, see [“Defining a classifier configuration” on page 854](#) and [“Defining a classifier field” on page 165](#).

Currency data type

The currency data type accepts numeric values with decimal places for currency values.

For more information, see [“Defining currency fields” on page 166](#).

Date data type

The date data type default value is blank and this value cannot be changed. The date picker pop-up box defaults to the current date.

For more information, see [“Defining a date field” on page 169](#).

Decimal data type

The decimal data type accepts numeric values with decimal places. A value range and default value can optionally be specified. If a user enters a value that is either below or above the specified value range or a non-decimal value, an error message is shown.

For more information, see [“Defining decimal fields” on page 169](#).

Enumerated String data type

The enumerated string data type accepts a list of string values. Define the values for the list and whether multiple values can be selected. A default value can optionally be specified.

For more information, see [“Defining enumerated string fields” on page 170](#).

Integer data type

The integer data type accepts numeric values without decimals. A value range and default value can optionally be specified. If a user enters a value that is either below or above the specified value range or a non-integer value, an error message is shown.

For more information, see [“Defining integer fields” on page 171](#).

Long String data type

A long string is considered to be any text of length more than 4000 bytes. Long strings allow users to enter more than 4000 bytes in a single field.

You can encrypt long string field values up to a maximum of 2 MB in the IBM OpenPages with Watson repository.

The long string data type has the following subtypes:

- Medium

Medium is a fixed size of 32 KB. Medium is the only size that is supported for FastMap uploads.

- Large

Large is a default size of 256 KB. It can be increased by changing the **Platform > Repository > Resource > Large Text > Maximum Size** setting. Enter a value in bytes. The maximum size applies to all large subtype long strings.

Important: After it is set, this value cannot be reduced.

Note: The maximum size is a hidden setting. To show hidden settings set **Applications > Common > Configuration > Show Hidden Settings** to **true**.

The display type determines how a long string field is presented to the user.

Long string fields can have the following display types:

- Rich Text

Provides a text display area with a toolbar and commands for text formatting and word processing. The toolbar can be minimized or expanded. The space used for non-printing, formatting, and multi-byte characters might cause the data to exceed the size of the medium long string field, resulting in an error message.

- Text Area

Provides a box display area in which users can enter either plain or HTML-formatted text.

Reporting Fragment data type

The Reporting Fragment data type displays a component (such as a bar or line chart) from a Cognos report or dashboard in a field. For more information, see [“Configuring reporting fragment fields” on page 176](#).

Simple String data type

The simple string data type, by default, displays data as text. The default value of the field is blank. The maximum size of a simple string is 4000 bytes.

You can encrypt simple string field values in the IBM OpenPages with Watson repository. You can also provide a default value.

The display type determines how the field is presented to the user.

Simple string fields can have the following display types:

- Link

Contains a URL value. It validates that the web address is a fully qualified URL internet address (for example, `http://www.mycompany.com` or `ftp://ftp.myftpsite.com`) and will display an error message to the user if the format of the web address is incorrect.

- Rich Text

Provides a text display area with a toolbar and commands for text formatting and word processing. The toolbar can be minimized or expanded. You may not be able to enter 4000 rich text characters into the text display area because of the space used for formatting and multi-byte characters.

- Text

Provides a box area in which users can enter a string value.

Note: When generating reports in PDF format, rich text fields do not render properly and the format is not preserved.

- Text Area

Provides a box display area in which users can enter either plain or HTML-formatted text.

After it is defined, you cannot change a field defined as simple string data type to long string data type.

For more information, see [“Defining simple string fields” on page 172](#).

User/Group data type

The User/Group data type allows the selection of users and/or groups. The display type controls whether the field is for users and/or groups and whether single or multiple selections can be made.

A User/Group field can have the following display types:

- Group Selector

Allows the selection of a single user group.

- Multi-valued Group Selector

Allows the selection of multiple user groups.

- Multi-valued User Selector

Allows the selection of multiple users.

- Multi-valued User/Group Selector

Allows the selection of multiple users and/or groups.

- User Selector

Allows the selection of a single user.

- User/Group Selector

Allows the selection of a single user or group.

The following additional settings for user/group fields are defined on the profile:

- Include Disabled
- Starting Group
- Include Subgroups

Colors for field value ranges

You can apply colors to value ranges for decimal, integer, and currency fields.

Colors can be applied to field value ranges, and they are displayed in all views that contain the field.

For a list of color values, see [“Supported color palettes for field values” on page 159](#).

For currencies, the color that is applied is based on the base currency. For example, if the local amount is 20 EUR and the base currency is USD and the exchange rate is 2, the applied color is based on 40 USD.

When you build color ranges, the following rules apply:

- Overlaps in range values are not allowed.
- If you choose no color (the white cell), the value renders as gray.
- A typical definition of a color range has no gaps in the range values, and the top value of one range is equal to the bottom value of the next range.
- If there are gaps in ranges, the value renders as gray.

- In general, the first value in a range is inclusive and the last value is exclusive. This enables the system to correctly apply colors to decimal values. An exception exists for the last value of the highest possible range, which is always inclusive so that a color is applied to the maximum value of a field.

The following example shows how colors are rendered for a typical color range.

<i>Table 78. Example for a field that has a maximum value of 100</i>		
Range	Color	Result
0-25	Green	0 and all values up to but not including 25 display as green.
25-50	Yellow	25 and all values up to but not including 50 display as yellow.
50-100	Red	50 and all values up to and including 100 display as red.

If the same field had a maximum value of infinity, the colors are applied as follows:

<i>Table 79. Example for a field that has no defined maximum value</i>		
Range	Color	Result
0-25	Green	0 and all values up to but not including 25 display as green.
25-50	Yellow	25 and all values up to but not including 50 display as yellow.
50-100	Red	50 and all values up to but not including 100 display as red.
100 to infinity	Dark Red	100 and all values above 100 display as dark red.

For more information about how to apply colors to field value ranges, see [“Defining fields and adding them to field groups” on page 161](#).

Supported color palettes for field values

Available colors for field values are based on two Carbon color palettes, Categorical and Monochromatic.

When you apply colors to enumerated fields and fields in charts, colors can be chosen from either the Categorical or the Monochromatic palette. The palettes have been designed to be aesthetically inviting for users. They also maximize contrast between the background color and the colors of the UI elements so that they are compliant with accessibility standards.

The Categorical palette has a light and dark set of colors, which are based on the light and dark themes. When you are defining views and charts, the theme that is applied to the signed on user determines the colors that are available in the categorical palette. If the signed on user is using a light theme, the light color set in the Categorical palette is displayed. If the signed on user is using a dark theme, the dark color set in the Categorical palette is displayed.

How colors display to a user depends on the theme that they're using. The system finds the closest match between how the field or chart was defined and how the theme is defined.

In previous versions, a fixed list of colors was supported. The system finds the closest match between those colors and the Carbon palette colors. Fields must not be redefined. However, you might want to review your field colors and take advantage of the palettes to improve the system to be more visually aesthetic and to meet accessibility standards.

For more information about how to apply colors to field values and value ranges, see [“Defining fields and adding them to field groups” on page 161](#).

For more information about themes, see “Themes” on page 241.

For more information about the palettes, see the following Carbon documentation:

- <https://www.carbondesignsystem.com/data-visualization/color-palettes/>
- <https://www.carbondesignsystem.com/guidelines/color/usage/>

Design tab

On the **Design** tab, if you choose no color (the white cell), the value renders as transparent.

JSON tab

On the JSON tab, a color is defined in a *color* property.

Defining field groups

Field groups are containers that organize fields into logical groups.

About this task

Use this task to create a new field group and then add a field to it.

Procedure

1. Enable System Admin Mode. For more information, see [“Enabling and disabling System Admin Mode” on page 37](#).
2. Click  > **Solution Configuration** > **Object Types**.
3. Select an object type.
4. Expand the **Fields** section.
5. To create a field group, click **New Field**.
6. Click **New** next to **Field Group**.
7. Enter a **Name** and **Description** and click **Create**.
The name must start with a letter, and can contain only letters, numbers, spaces, hyphens (-), and the underscore (_) character.
8. Continue defining the new field.
9. Click **Create**.

What to do next

Add field definitions to the new field group. For details, go to [“Defining fields and adding them to field groups” on page 161](#).

Adding existing field groups to object types

A field group can be assigned to multiple object types, which allows you to more easily manage and share common fields across multiple object types.

About this task

Use this task to assign and unassign an existing field group to an object type. You can also change a field group description and create new fields.

Procedure

1. Enable System Admin Mode. For more information, see [“Enabling and disabling System Admin Mode” on page 37](#).

2. Click  > **Solution Configuration** > **Object Types**.

3. Select an object.

4. Expand the **Field Groups** section.

Field groups that are already assigned to the object type are listed.

5. To add an existing field group to the object type, click **Add Field Groups**.

a) In **Field Groups**, select all the field groups to add to the object type.

b) In **Add fields to Profiles**, select one or more profiles. The fields in the field groups are added to the profiles that you select.

Tip: If you want to add some fields to some profiles and other fields to other profiles, you can use the **Profiles** page to add or remove fields from a profile. For more information, see “[Including fields in an object type](#)” on page 227 and “[Excluding fields from an object type](#)” on page 228.

c) Click **Done**.

6. To modify a field group, select a field group.

a) Change the description, if needed.

b) Click **New Field** to create a field. For more information, see “[Defining fields and adding them to field groups](#)” on page 161.

c) Click **Done**.

Defining fields and adding them to field groups

A field definition stores the data type and other properties of a field.

For each new field to add to an object type, you must create a field definition that defines the properties of that field. You can add a field definition to an existing field group or create a new field group.

Before you begin

Learn about data types and display types. For more information, see “[Data types](#)” on page 155.

If the field group is already associated to an object type and you use IBM Db2 and the reporting schema is enabled, perform this task when there is limited or no activity on the system. It can cause significant system delays in OpenPages due to locking conflicts on the Db2 platform. For more information, see “[System delay when modifying object types and fields \(Db2\)](#)” on page 947.

Procedure

1. Enable System Admin Mode. For more information, see “[Enabling and disabling System Admin Mode](#)” on page 37.

2. Click  > **Solution Configuration** > **Object Types**.

3. Click an object type.

4. Expand the **Fields** section to work with fields and field groups.

5. Click **New Field**.

6. In **Field Group**, select the field group that the new field is assigned to.

Or, click **New** to create a new field group. Enter a **Name** and **Description** and click **Create**.

7. Enter a **Name**. The name must start with a letter, and can contain only letters, numbers, spaces, hyphens (-), and the underscore (_) character. After it is defined, you cannot change a field's name. You can, however, change the label.

8. Enter a **Label**. Click **Edit** to add values in multiple languages.

9. Enter a **Description**.

10. Select a **Data Type** and complete the fields that are specific to that data type.

Table 80. Data Types

For this data type...	See this topic...
Boolean	“Defining Boolean fields” on page 164
Business Entity Selector	“Defining business entity selector fields” on page 165
Classifier	“Defining a classifier field” on page 165
Currency	“Defining currency fields” on page 166
Date	“Defining a date field” on page 169
Decimal	“Defining decimal fields” on page 169
Enumerated String	“Defining enumerated string fields” on page 170
Integer	“Defining integer fields” on page 171
Long String	“Defining long string fields” on page 172
Reporting Fragment	“Configuring reporting fragment fields” on page 176
Simple String	“Defining simple string fields” on page 172
User/Group	“Defining user/group fields” on page 173

11. Set **Required** to True or False. For more information, see [“Making fields required or optional” on page 162](#).

12. Set **Global Search** to True or False.

Note: Fields that are encrypted are not eligible for use in Global Search.

Enabling Global Search for simple or long string fields that have field level security might result in users being able to derive data values they otherwise would not have access to. For more information, see [“Field level security” on page 92](#).

13. Optional: If **Data Type** is **Currency**, **Decimal**, or **Integer**, you can set value ranges and apply colors to them. For more information, see [“Defining currency fields” on page 166](#), [“Defining decimal fields” on page 169](#), or [“Defining integer fields” on page 171](#) depending on the data type of the field.

14. Optional: If **Data Type** is **Enumerated String**, you can set values and apply colors to them. For more information, see [“Defining enumerated string fields” on page 170](#).

15. Optional: If **Default Value** is displayed, you can set a default value for the field. For more information, see [“Setting a default value for an object field” on page 164](#).

16. Expand **Profiles**. From the **Object Profiles** list, select the profiles that can use the field. By default, all profiles that the object type belongs to are selected.

17. Click **Create**.

18. Add more fields to the field group, as needed.

19. To edit a field, click a field row.

a) Edit settings on the field. Click **Edit** next to **Label** to update label values. Description can also be edited. Not all fields can be changed, for example, the **Name** cannot be changed. The settings that are displayed depend on the field type.

b) Expand **Profiles**. View and change the profile that the field is assigned to.

c) Click **Done**.

Making fields required or optional

You can globally set whether all users are required to enter data in an object field.

When you create a new object field, by default, the **Required** setting is False, which means the field is optional or non-required during data entry.

Note: If you want to require a specific group of users (not all users) to enter data for a field, for maximum flexibility set the field as required in the profile and not in the field definition (see “[Setting a field in a profile to required or optional](#)” on page 228).

When you set an object field to be required, a red asterisk * displays after the field label. For example, if you were to change the setting of the optional “Additional Description:” field of the Account object to be a required data entry field, it displays to users as “Additional Description*:”. Users are required to enter information in the field when they created a new Account object.

You can omit a required field for a particular view if the field is filled in by a trigger or if the field will have been filled in prior to this view being used to edit the object.

Procedure

1. Define basic information about the field. For more information, see “[Defining fields and adding them to field groups](#)” on page 161.
2. Set **Required**:
 - True - the field is required
 - False - the field is optional
3. Finish defining the field. For more information, see “[Defining fields and adding them to field groups](#)” on page 161.

What to do next

Note: Changing a field to Required also causes all profile references to the field to be required as well.

Encrypting field values

You can encrypt a simple string or long string field value in the IBM OpenPages with Watson repository to prevent system administrators from viewing confidential data directly from the database. Encrypted field values are shown as a string of random characters.

Note: Before encrypting long strings in OpenPages running on Oracle 12.2, refer to the following Technote: <http://www.ibm.com/support/docview.wss?uid=swg22010106>. The Technote describes a potential issue and how to resolve it by obtaining the appropriate patch from Oracle support and applying it to your environment.

Procedure

1. Define basic information about the field. For more information, see “[Defining fields and adding them to field groups](#)” on page 161.
2. To encrypt all values for the field, set **Encrypted** to True.
3. Finish defining the field. For more information, see “[Defining fields and adding them to field groups](#)” on page 161.

Results

The field is now marked for encryption. The timing of the encryption depends on the status of the field level encryption keystore:

- If keystore is enabled, all field values are encrypted when you save the field definition.
- If the keystore is disabled, no field values are encrypted until you enable the keystore.

For more information, see [“Configure field level encryption” on page 110](#).

Decrypting field values

You can decrypt a simple string or long string field value in the IBM OpenPages with Watson repository if the data is no longer considered to be confidential. System administrators can view decrypted data directly from the database.

Procedure

1. Define basic information about the field. For more information, see [“Defining fields and adding them to field groups” on page 161](#).
2. To decrypt all values for the field, set **Encrypted** to False.
3. Finish defining the field. For more information, see [“Defining fields and adding them to field groups” on page 161](#).

Results

The field is now marked for decryption. The timing of the decryption depends on the status of the field level encryption keystore:

- If the keystore is enabled, no field values are decrypted until you disable the keystore.
- If keystore is disabled, all field values are decrypted when you save the field definition.

For more information, see [“Configure field level encryption” on page 110](#).

Setting a default value for an object field

When you create a new object field, by default, the **Default Value** property is empty (not populated).

When you set a default value for an object field, that value displays to users in that field. For example, if you were to set a default value for the “Additional Description:” field of the Account object that contained the text “Enter any additional information here.”, it displays to users when they created a new Account object.

Restriction: The new default value will only be populated for new instances of an object type. In other words, if a user attempts to edit an existing object where the value was blank, it will remain blank. The new default value will be used when a user or administrator creates a new instance of that object type. For example, if an administrator modifies an enumerated string (dropdown field) on a test object. The new default value will be populated if new test objects are created. If an end user attempts to edit an existing test object, the new default value won’t be set or modified for it.

Procedure

1. Define basic information about the field. For more information, see [“Defining fields and adding them to field groups” on page 161](#).
2. In **Default Value**, either type a value or select a value.
3. Finish defining the field. For more information, see [“Defining fields and adding them to field groups” on page 161](#).

Defining Boolean fields

Define a Boolean field by setting the data type and a default value.

Before you begin

Learn about the data type. For more information, see [“Data types” on page 155](#).

Procedure

1. Define basic information about the field. For more information, see [“Defining fields and adding them to field groups” on page 161](#).
2. Select Boolean in **Data Type**.
3. Select True or False in **Default Value**.
4. Finish defining the field. For more information, see [“Defining fields and adding them to field groups” on page 161](#).

Defining business entity selector fields

Define a business entity selector field by setting the data type and additional settings on profiles.

Before you begin

Learn about the data type. For more information, see [“Data types” on page 155](#).

Procedure

1. Define basic information about the field. For more information, see [“Defining fields and adding them to field groups” on page 161](#).
2. Select Business Entity Selector in **Data Type**.
3. Finish defining the field. For more information, see [“Defining fields and adding them to field groups” on page 161](#).

What to do next

Click  > **Solution Configuration** > **Profiles**. Select a profile to modify and a business entity selector field. Set the following values:

Table 81. Business Entity Selector options on profiles	
Setting	Description
Starting Business Entity	The default value for Starting Business Entity is a forward slash (/). If you want all Level 1 business entities displayed, retain the default. To set a starting business entity, navigate through the business entity tree and select a business entity.
Number of Levels	Determines the number of levels that end users can navigate to from the starting business entity. For example, if you select Global Financial Services as your starting business entity and set the number of levels to 2, you can navigate to two levels below Global Financial Services (Global Financial Services/Asia Pac/Agency Services). Limit the number of levels to improve performance of the selector and help users select from the entities most appropriate for this field. The default value is 3.

Defining a classifier field

Define a classifier field by setting the data type and additional settings.

Procedure

1. Define basic information about the field. For more information, see [“Defining fields and adding them to field groups” on page 161](#).

2. Select Classifier in **Data Type**.
3. Select a **Classifier Configuration Name**. The name of a classifier configuration defined in  > **Integrations > Mapping and Taxonomy Suggestions**.
4. In **Classifier Input Field**, click **Set** and select a field group and field. The field that provides text that is interpreted and classified by a natural language processing service.
5. Finish defining the field. For more information, see “[Defining fields and adding them to field groups](#)” on [page 161](#).

Defining currency fields

Define a currency field by setting the data type, Include Conversion, a value range, and defining additional settings on profiles.

Before you begin

Learn about the data type. For more information, see [“Data types” on page 155](#).

About this task

- The Minimum Value and Maximum Value settings are expressed in terms of the base currency (base currency is set during installation). If a user enters a value that is either below or above the value range, an error message is shown.
- You cannot use non-numeric characters when you enter currency values. For example, either 125000 or 125,000 is legal, but not \$125000. This format is set per user locale.
- Object fields with this data type cannot be included in the profile of predefined objects that use the supplied JSP file for rendering.

Note: The Currency data type does not support computed fields. See [“Defining a computed field” on page 183](#) for information on computed fields.

Procedure

1. Define basic information about the field. For more information, see [“Defining fields and adding them to field groups” on page 161](#).
2. Select Currency in **Data Type**.
3. Set **Include Conversion** to True or False to control whether the exchange rate and base amount conversion are visible.
 - **True** (default) - the following items are displayed to the user when they work with the currency field:
Local Currency Code (drop down)
Local Amount (text input)
Exchange Rate (text input)
Base Code (static text)
Base Amount (static text)

For example, you might use this setting when the field represents a currency amount relative to a specific point in time where the exchange rate is applicable, such as a financial loss on a specific date.

- **False** - the following items are displayed to the user when they work with the currency field:

Local Currency Code (drop down)
Local Amount (text input)

For example, you might use this setting when the field represents a hypothetical currency amount not relative to a specific point in time, such as Inherent Severity on the Risk object.

4. Optional: In **Minimum Value** enter the lowest value that is allowed.
5. Optional: In **Maximum Value** enter the greatest value that is allowed.
6. Optional: You can define ranges of values and apply colors to each range.

Following the paragraph that states **Bottoms of ranges are inclusive. Tops of ranges are exclusive,**

except for the highest possible range., click  to start building ranges. Choose a color for each range of values for the field. The available colors depend on the color palette you selected.

If you choose no color (the white cell), the value renders as gray.

For more information about applying range values and colors, see “[Colors for field value ranges](#)” on page 158.

7. Expand **Profiles**. From the **Object Profiles** list, select the profiles that can use the field. By default, all profiles that the object type belongs to are selected.
8. Click **Done**.

What to do next

Click  > **Solution Configuration** > **Profiles**. Select a profile to modify and a currency field. Set the following value:

<i>Table 82. Currency field settings on profiles</i>	
Setting	Description
Exchange Rate Read Only	<p>Controls whether exchange rates for the currency are read only.</p> <p>If the Exchange Rate Read Only value is set to:</p> <ul style="list-style-type: none"> • True - exchange rates for the currency are read only • False - exchange rates for the currency are not read only

Modifying currency exchange rates

You can add, edit, enable, and disable currency exchange rates.

Ensure that your user has the **SOX > Administration > Currencies** application permission.

Use one of the following methods to update currency exchange rates.

- Upload a CSV file with currency exchange rates from:
 - The **Currencies** task. For more information, see “[Editing, enabling, disabling, and uploading currency exchange rates](#)” on page 168.
 - An ObjectManager loader file. For more information, see “[Importing exchange rates](#)” on page 752.
- Edit the rates manually. For more information, see “[Editing, enabling, disabling, and uploading currency exchange rates](#)” on page 168.
- Upload currency exchange rates in an ObjectManager loader file. For more information, see “[Importing exchange rates](#)” on page 752.

Note: You cannot use these functions with a new currency. The currency must exist.

Formatting a CSV file

The file containing the exchange rate currency data must be in a comma separated value (.csv) file that is formatted in a specific way.

The file must have the following format:

```
<currency code>,<exchange rate>
<currency code>,<exchange rate>
```

Where:

Table 83. CSV file format placeholders for exchange rates	
Field	Description
<currency code>	The 3-letter ISO Currency Code.
<exchange rate>	The numeric exchange rate value. The default value is 1.0.
<start date>	Optional. The date the exchange rate was (or will be) applied. You can use either of the following formats: <ul style="list-style-type: none">• mm/dd/yyyy• mm/dd/yyyy HH:mm:ss If no historic date is supplied, the current date is used.

The following data sample from a CSV file shows the ISO currency codes for Euros, Canadian dollars, and Japanese yen with the corresponding exchange rate for each currency, and the historical date that the rate was applied for two of the three currencies.

```
EUR,0.1589,12/26/2007
CAD,0.8636
JPY,0.0083,5/8/2008
```

The number of rows in the CSV file might be limited. For more information, see [“Maximum rows in exchange rate upload file” on page 500](#).

Editing, enabling, disabling, and uploading currency exchange rates

You can edit, enable, and disable currency exchange rates. You can also upload exchange rates from a CSV file.

Before you begin

To upload exchange rates, create the CSV file. For more information, see [“Formatting a CSV file” on page 167](#).

About this task

You can enable disabled currency rates, making them available to the appropriate processes.

You can disable enabled currencies. When you disable a currency it is no longer available to the system. However, it is not deleted. You can enable it at any time.

Note: You cannot enable or disable the base currency, which is set during installation.

Procedure

1. Click  > **System Configuration** > **Currencies**.
2. To view a currency and its exchange rates, select it.

3. To upload a CSV file, deselect all currencies and click **Upload**. Select a file and click **Upload**.
The new currency exchange rate appears in the list of enabled currencies.
4. To manually edit the exchange rates for one or more currencies, deselect all currencies and click **Edit**.
Edit the exchange rates and click **Save**. For each change, a new exchange rate with today's timestamp is created.
5. To enable a currency, deselect all currencies and click **Enable**. All currencies are listed. Select the currencies that you want to enable and click **Enable**.
The currency appears in the list of enabled currencies.
6. To disable a currency, select it and click **Disable**.
The currency is no longer shown in the list of enabled currencies.

Defining a date field

Define a date field by setting the data type.

Before you begin

Learn about the data type. For more information, see [“Data types” on page 155](#).

Procedure

1. Define basic information about the field. For more information, see [“Defining fields and adding them to field groups” on page 161](#).
2. Select Date in **Data Type**.
3. Finish defining the field. For more information, see [“Defining fields and adding them to field groups” on page 161](#).

Defining decimal fields

Define a decimal field by setting the data type, a value range, and a default value.

Before you begin

Learn about the data type. For more information, see [“Data types” on page 155](#).

Procedure

1. Define basic information about the field. For more information, see [“Defining fields and adding them to field groups” on page 161](#).
2. Select Decimal in **Data Type**.
3. Optional: In **Minimum Value** enter the lowest decimal value that is allowed.
4. Optional: In **Maximum Value** enter the greatest decimal value that is allowed.
The maximum number of digits you can use is 16.
5. Optional: You can define ranges of values and apply colors to each range.

Following the paragraph that states **Bottoms of ranges are inclusive. Tops of ranges are exclusive**, **except for the highest possible range**, click  to start building ranges. Choose a color for each range of values for the field. The available colors depend on the color palette you selected.

If you choose no color (the white cell), the value renders as gray.

For more information about applying range values and colors, see [“Colors for field value ranges” on page 158](#).

6. Optional: In **Default Value** enter a numeric value that is between the minimum and maximum allowable values.

7. Expand **Profiles**. From the **Object Profiles** list, select the profiles that can use the field. By default, all profiles that the object type belongs to are selected.
8. Click **Done**.

Defining enumerated string fields

Define an enumerated string field by setting the data type, adding values, applying colors to the values, and defining whether it is encrypted and single or multi-valued. A default value can also be specified.

Before you begin

Learn about the data type. For more information, see “[Data types](#)” on page 155.

About this task

You can apply colors to the values for an enumerated string field.

For a list of color values, see “[Supported color palettes for field values](#)” on page 159.

In the following example, color was applied to values for the Design Effectiveness and Operating Effectiveness fields. The example shows how the field values are displayed. Note that Effective and Not Determined are enumerated string values, not translated labels.

Figure 12. Example of colors applies to enumerated value fields



Procedure

1. Define basic information about the field. For more information, see “[Defining fields and adding them to field groups](#)” on page 161.
2. Select Enumerated String in **Data Type**.
3. Set **Multi Valued**:
 - True - multiple values can be selected from the list.
 - False - only one value can be selected from the list (the default).
4. Add values to the list:
 - a) In **Enumerated String Values** click **New Value**.
 - b) Enter a **Name** and a **Label**.
 - To add labels in multiple languages, click **Edit**.
 - c) Click **Create**.
5. To reorder the values in the list, use drag and drop and position the values in the correct display order.
6. Hover over a value and click the show/hide icon to control whether a value is displayed to users.
7. To remove a value from the list, click the remove icon next to the value.
8. Optional: You can apply colors to the values.
 - a) Choose **Categorical** or **Monochromatic** in **Color Palette**.
 - b) In **Color Values**, choose a color for each enumerated value for the field. The available colors depend on the color palette you selected.
 - If you choose no color (the white cell), the value renders as gray.
 - c) Click **Create**.
9. Optional: In **Default Value** select a value that is the default.

10. Expand **Profiles**. From the **Object Profiles** list, select the profiles that can use the field. By default, all profiles that the object type belongs to are selected.
11. Click **Done**.

Results

After an enumerated field, either single or multi-valued, is created, a true/false toggle named **Hierarchical** might be displayed. It is an internal setting and cannot be changed.

After it is defined, you cannot change an enumerated string field from a multi-value enumerated string data type to single-value enumerated data type. You cannot delete an enumerated string field.

If you are using Oracle, you can convert a single value selection setting to a multi-value selection setting.

If you are using IBM Db2 and you want to convert a single value selection setting to a multi-value selection setting, you must:

- Perform the conversion when there is limited or no activity on the system if the reporting schema is enabled. The conversion can cause significant system delays in OpenPages due to locking conflicts on the Db2 platform. For more information, see [“System delay when modifying object types and fields \(Db2\)” on page 947](#).
- Complete remediation steps after the conversion is finished. For more information, see [“Remediating after an Enumerated String field is changed to a multi-select field \(Db2\)” on page 947](#). Or, drop the reporting schema, change the setting, and then re-create the reporting schema.

Defining integer fields

Define an integer field by setting the data type, a value range, and a default value.

Before you begin

Learn about the data type. For more information, see [“Data types” on page 155](#).

Procedure

1. Define basic information about the field. For more information, see [“Defining fields and adding them to field groups” on page 161](#).
2. Select Integer in **Data Type**.
3. Optional: In **Minimum Value** enter the lowest integer value that is allowed.
4. Optional: In **Maximum Value** enter the greatest integer value that is allowed.
5. Optional: You can define ranges of values and apply colors to each range.

Following the paragraph that states **Bottoms of ranges are inclusive. Tops of ranges are exclusive, except for the highest possible range.**, click  to start building ranges. Choose a color for each range of values for the field. The available colors depend on the color palette you selected.

If you choose no color (the white cell), the value renders as gray.

For more information about applying range values and colors, see [“Colors for field value ranges” on page 158](#).

6. Optional: In **Default Value** enter an integer value that is between the minimum and maximum allowable values.
7. Expand **Profiles**. From the **Object Profiles** list, select the profiles that can use the field. By default, all profiles that the object type belongs to are selected.
8. Click **Done**.

Defining long string fields

Define a long string field by setting the data type, string size, display type, encryption, and providing a default value.

Before you begin

Learn about the data type. For more information, see [“Data types” on page 155](#).

Procedure

1. Define basic information about the field. For more information, see [“Defining fields and adding them to field groups” on page 161](#).
2. Select Long String in **Data Type**.
3. Select a **String Size**:
 - Medium
 - Long
4. Select a **Display Type**:
 - Rich Text
 - Text Area
5. Set **Encrypted** to True or False.

Long string fields that are encrypted:
 - are not eligible for use in Global Search.
 - display a blank result when used as filter criteria.For more information, see [“Encrypting field values” on page 163](#) and [“Decrypting field values” on page 164](#).
6. Finish defining the field. For more information, see [“Defining fields and adding them to field groups” on page 161](#).

Defining simple string fields

Define a simple string field by setting the data type, string size, display type, encryption, and providing a default value.

Before you begin

Learn about the data type. For more information, see [“Data types” on page 155](#).

Procedure

1. Define basic information about the field. For more information, see [“Defining fields and adding them to field groups” on page 161](#).
2. Select Simple String in **Data Type**.
3. Select a **Display Type**.

Valid values for simple strings are:

 - Link
 - Rich Text
 - Text
 - Text Area
 - Show full list of display types

Do not create new fields with the Show full list of display types option. Use this option only for imported fields that have no display type. This can happen if a field is imported that did not have an assigned profile in the same configuration file.

4. Set **Encrypted** to True or False.

Simple string fields that are encrypted:

- are not eligible for use in Global Search.
- cannot be defined to use security rules (both record level and field level). For more information, see “[Security rules](#)” on page 80.

For more information, see “[Encrypting field values](#)” on page 163 and “[Decrypting field values](#)” on page 164.

5. Enter a **Default Value**. Type a string of either plain text or HTML-formatted text.

For more information, see “[Setting a default value for an object field](#)” on page 164.

6. Finish defining the field. For more information, see “[Defining fields and adding them to field groups](#)” on page 161.

Defining user/group fields

Define a user/group field by setting the data type, display type, and defining additional settings on profiles.

Before you begin

Learn about the data type. For more information, see “[Data types](#)” on page 155.

Procedure

1. Define basic information about the field. For more information, see “[Defining fields and adding them to field groups](#)” on page 161.

2. Select User/Group in **Data Type**.

3. Select a **Display Type**.

Valid values for user/group fields are:

- **Group Selector**: Allows the selection of a single user group.
- **Multi Valued Group Selector**: Allows the selection of multiple user groups.
- **Multi Valued User Selector**: Allows the selection of multiple users.
- **Multi Valued User/Group Selector**: Allows the selection of multiple users and/or groups.
- **User Selector**: Allows the selection of a single user.
- **User/Group Selector**: Allows the selection of a single user or group.

4. Finish defining the field. For more information, see “[Defining fields and adding them to field groups](#)” on page 161.

What to do next

Improve the performance of user/group fields by setting additional fields on profiles.

If your deployment has a large number of users, the performance of the User Selector or the Multi-Valued User Selector in opening and loading data may be sluggish. One way to improve the performance of the User Selector or the Multi-Valued User Selector is to configure it so it retrieves only users who have permission on the object being edited. You do this by setting **Minimum Access** on profiles.

The supplied profiles in the IBM OpenPages with Watson application are configured such that the User Selector or Multi-Valued User Selector pop-up retrieves all users in the system - including some application users who do not have security permissions on the selected object. This might result in the assignment of a user as “owner” on an object when the user does not have read access on the object.

Set **Minimum Access** to restrict the set of users retrieved by the User Selector or the Multi-Valued User Selector to those users that have access permissions on the object being edited at the time.

Click  > **Solution Configuration** > **Profiles**. Select a profile to modify and a user/group field. Set the following values:

<i>Table 84. Additional selector settings</i>	
Setting	Description
Include Disabled	<p>Allows or disallows disabled user accounts to be included in a selector listing.</p> <p>If the Include Disabled value is set to:</p> <ul style="list-style-type: none"> • True - disabled user accounts are included in the selector listing. When this setting is selected, the Minimum Access setting is disabled. A value of True, when used in combination with a Starting Group value that contains many users, can result in slower search performance. • False - disabled user accounts are excluded from the selector listing. When this setting is selected, the Minimum Access setting is enabled. <p>This setting generally applies to User (not Group) selectors.</p>
Starting Group	<p>Controls which group displays at the beginning of the selection hierarchy.</p> <p>If the Starting Group value is blank, selectors search the system for all users and/or groups, depending on the display type. A blank Starting Group value used in combination with an Include Disabled value of True can result in improved search performance.</p> <p>To select a starting group, click the group icon and select a valid group name from the selector window.</p> <p>For example, if you are using role-based security, you could select the Security Domains group, for non role-based security, you could select the Workflow, Reporting and Others group.</p>
Include Subgroups	<p>Controls whether subgroups are included or excluded from the User selector listing.</p> <p>Note: This setting applies only to the User/Group and Group selectors.</p> <p>If the Include Subgroups value is set to:</p> <ul style="list-style-type: none"> • True - subgroups are included in the selector listing. • False - subgroups are excluded from the selector listing.

Table 84. Additional selector settings (continued)

Setting	Description
Minimum Access <ul style="list-style-type: none"> • Read • Write • Delete • Associate 	<p>This setting is enabled only if the Include Disabled value is set to False. This setting allows you to filter users based on access control list settings on an object's folder.</p> <p>For example, you want to limit the number of users who can be assigned as a Process "Cycle Owner", which is an object field with a user selector display type for the Process object. Because you previously set up an access control list (ACL) for one or more groups or users to the Process folder, you can use the Minimum Access setting to filter the list of users. If you only wanted users with "Delete" permissions to be displayed on the user selector list, you can select the "Delete" Minimum Access setting to filter and display only those users with "Delete" ACL permissions.</p> <p>If the Read box is:</p> <ul style="list-style-type: none"> • Selected - only users with Read access are displayed on the user list. • Cleared - no filtering occurs. <p>If the Write box is:</p> <ul style="list-style-type: none"> • Selected - only users with Write access are displayed on the user list. • Cleared - no filtering occurs. <p>If the Delete box is:</p> <ul style="list-style-type: none"> • Selected - only users with Delete access are displayed on the user list. • Cleared - no filtering occurs. <p>If the Associate box is:</p> <ul style="list-style-type: none"> • Selected - only users with Associate access are displayed on the user list. • Cleared - no filtering occurs.

Changing the display type for users and groups

If you change the display type of the actor fields in a profile, you must take action on the filters.

About this task

Table 85. Display type changes that require action

If you change this display type	To this display type	Take this action ¹
User Selector	Group Selector or Multi Valued Group Selector	A
	User/Group Selector or Multi Valued User/Group Selector	B
User Dropdown (legacy)	Group Selector or Multi Valued Group Selector	A

Table 85. Display type changes that require action (continued)

If you change this display type	To this display type	Take this action ¹
	User/Group Selector or Multi Valued User/Group Selector	B
User/Group Selector	Group Selector or Multi Valued Group Selector	A
	User/Group Selector or Multi Valued User/Group Selector	B
Group Selector	Multi Valued Group Selector	A
	User/Group Selector or Multi Valued User/Group Selector	B
Multi-Valued User Selector	Multi Valued Group Selector	A
	Multi Valued User/Group Selector	B
Multi-Valued Group Selector	Multi Valued User/Group Selector	A
Multi-Valued User/Group Selector	Multi Valued Group Selector	A

¹ Actions

- A: If you make this change, and if "End User" is set as the filter value for that actor field in the filter, the "End User" must be updated to the group so that the filters can return the expected results.
- B: If you make this change, re-save the filter so that it can return the expected results.

If you specified a default value for the field, the default value is cleared when you change the display type. Reset the default value of the field.

If you set or change the display type of a field to **Multi Valued User Selector** or **Multi Valued Group Selector** or **Multi Valued User/Group Selector**, update the reporting schema. For more information, see "Updating the reporting schema" on page 121.

You cannot change a **Multi Valued User Selector**, **Multi Valued Group Selector**, or **Multi Valued User/Group Selector** display type to a single actor display type.

Configuring reporting fragment fields

Reporting fragment fields are always read-only fields that typically display a component (such as a chart or table) from a larger Cognos report.

Reporting fragment fields are configured in a number of ways:

- Associate with an object type
- Add to views
- Configure as dependent fields
- Modify their display type

Reporting fragment fields that were defined in previous versions of OpenPages might contain Automatic or On Demand as a value for Display Type for views. The functionality behind On Demand is obsolete. All reporting fragment fields are now handled as automatic.

Limitations

Reporting fragment fields have the following limitations:

- You cannot use elements from JSP reports in reporting fragment fields; only components from Cognos reports are supported.
- Page breaks in reporting fragment fields are not supported.
- Tooltips in reporting fragment fields are not supported.
- A report that has required prompts other than Object ID and Reporting Period ID cannot be used as a reporting fragment field.

Note: See the *IBM OpenPages with Watson Report Author's Guide* for information about designing reports that can be used in reporting fragment fields.

Overall configuration for reporting fragment fields

The overall configuration of reporting fragment fields involves the following tasks.

Table 86. Overall configuration of reporting fragment fields	
Task Description	Related Topic
Identify the Cognos report and report component and the field group you want to use.	“Planning considerations for reporting fragment fields” on page 177
Add the field group to an object type if it is not already included.	“Adding existing field groups to object types” on page 160
Access Cognos and be ready to obtain the parameter information to copy to the new field.	“Obtaining information from Cognos” on page 179
In the IBM OpenPages with Watson application, define the reporting fragment field.	“Defining a reporting fragment field” on page 178
Select a profile and add the reporting fragment field to an object type in that profile.	“Including fields in an object type” on page 227
Add the reporting fragment field to views.	Chapter 14, “Views,” on page 247
Optionally, change the display characteristics.	“Defining a reporting fragment field” on page 178

Planning considerations for reporting fragment fields

Before you add a reporting fragment field, you need to identify the report with the component you want, and which object types, profiles, and object views will be associated with the reporting fragment field.

Planning your changes ahead of time helps to minimize the necessary work and prevents duplication of effort.

The following list will help you identify some of the questions you need to consider before you create a new reporting fragment field:

- Report component — What report component data does the user need to see to accomplish their task? Which Cognos report contains the component?
- Field group — Will new reporting fragment fields reside in new or existing field groups?
- Object type — Which object type will use the reporting fragment field or fields?

- Views – Which views will use the reporting fragment fields? Reporting fragment fields can be added to Grid Views, Creation Views, Task Views, and Admin Views.
- Display – How many reporting fragment fields will be included in a view?

Defining a reporting fragment field

Reporting fragment fields are always read-only fields that typically display a component (such as a chart or table) from a larger Cognos report.

The process of creating a new reporting fragment field for use in OpenPages involves obtaining information from Cognos and then defining a reporting fragment field where you copy Cognos parameter information and paste it into fields on the reporting fragment field definition in OpenPages

Before you begin

You must have administrative privileges set on your account so you can access:

- The IBM Cognos Analytics and IBM Cognos Analytics - Reporting for obtaining parameter information.
- The IBM OpenPages with Watson application for defining the new reporting fragment field.

Define the field group that the reporting fragment field belongs to. For more information, see [“Defining field groups” on page 160](#).

Access Cognos and be ready to copy information to the new reporting fragment field. For more information, see [“Obtaining information from Cognos” on page 179](#).

Procedure

1. Define basic information about the field. For more information, see [“Defining fields and adding them to field groups” on page 161](#).
2. Select Reporting Fragment in **Data Type**.
3. Enter a **Report Path**. Enter the file path of the selected Cognos report that contains the component you want to use. Required.
Get this parameter value from the IBM Cognos Analytics, **Team content** folder.
For more information, see [“Obtaining the report path” on page 179](#).
4. Enter a **Fragment Name**. This is the unique name of the particular report component (such as a ‘Pie Chart’, ‘List’, ‘Combination Chart’, and so forth). Required.
Get this parameter value from the IBM Cognos Analytics - Reporting, Report Page.
For more information, see [“Obtaining the reporting fragment name” on page 179](#).
5. Enter an **Object ID Prompt**. It is required only if the report prompts users to select a resource (such as ‘Entity’, ‘Process’, and so forth) before running the report. Otherwise, leave this field blank.
Get this parameter value from the IBM Cognos Analytics - Reporting, Prompt Page.
For more information, see [“Obtaining the object ID prompt” on page 180](#).
6. Enter a **Reporting Period ID Prompt**. It is required only if the report prompts users to select a reporting period before running the report. Otherwise, leave this field blank.
Get this parameter value from the IBM Cognos Analytics - Reporting, Prompt Page.
For more information, see [“Obtaining the reporting period ID prompt” on page 181](#).
7. Enter the **Height** (in pixels) to manually control the size of the pop-window. If blank, the window is sized automatically.
8. Enter the **Width** (in pixels) to manually control the size of the pop-window. If blank, the window is sized automatically.
9. Finish defining the field. For more information, see [“Defining fields and adding them to field groups” on page 161](#).

Obtaining information from Cognos

Information must be obtained from Cognos before you can define reporting fragment fields in OpenPages.

Table 87. Cognos tasks	
Task	Required or optional
“Obtaining the report path” on page 179	Required.
“Obtaining the reporting fragment name” on page 179	Required.
“Obtaining the object ID prompt” on page 180	Required only if a report prompts users to select a resource (such as ‘Entity’, ‘Process’, and so forth) before running the report. Otherwise, skip this task and leave the field blank.
“Obtaining the reporting period ID prompt” on page 181	Required only if a report prompts users to select a reporting period before running the report. Otherwise, skip this task and leave the field blank.

Obtaining the report path

Obtain information from IBM Cognos Analytics so you can define **Report Path** on a reporting fragment field in OpenPages.

Procedure

1. Configure your environment to use the Cognos 10 home page, IBM Cognos Connection.
See [How to display the version 10 Cognos Connection home page in Cognos Analytics 11](#).
2. Open IBM Cognos Connection.
3. Click the **Team content** folder and navigate through the folder hierarchy to the report location.

For example,

Team content > OpenPages Solutions Reports > Risk Assessment Reports > Risk Assessment Status

4. In the **Actions** column for the report, click the **Set Properties** icon 
5. On the **Set Properties** page of the report, select **General**.
6. Click the **View the search path, ID and URL** link.
7. Copy the text in the **Search path** field.

The following example is a sample search path text for the Risk Assessment Status report.

```
/content/folder[@name='OPENPAGES_PLATFORM']/folder[@name='Risk Assessment Reports']/report[@name='Risk Assessment Status']
```

8. In OpenPages, go to the reporting fragment field definition and paste the search path text into **Report Path**.
9. Click **Launch > IBM Cognos Administration**.
10. Remove the portal.disablecc advanced setting that you added in step 1.

Obtaining the reporting fragment name

To obtain the name of the report component within the selected report, obtain information from IBM Cognos Analytics so you can define **Fragment Name** on a reporting fragment field in OpenPages.

Before you begin

Complete the following procedure to define the reporting fragment name:

Procedure

1. In IBM Cognos Analytics - Reporting, open the report containing the component you want:
 - a) On the **Team content** tab, navigate through the folder hierarchy to where the report you want is saved.

For example, Team content > OpenPages Solutions Reports > Risk Assessment Reports > Risk Assessment Status
 - b) Under the Actions column for the report you want, click **Edit report**.
2. In edit mode, select the component you want to use for the Reporting Fragment field (such as a List, a Chart, a Crosstab, and so forth.)
3. Verify that the entire component is selected:
 - a) Click **Show Properties** in the application bar.
 - b) In the **Properties** pane, look at the title bar. It should display the name of the selected component, such as Pie Chart, List, Combination Chart, and so forth.
 - c) If the Properties title bar displays the name of a subcomponent (for example List Column Body or List Column Title), then click the Properties up arrow icon on the Properties title bar and select the entire component (for example, List).
4. In the Properties pane, under the **Miscellaneous** heading, copy the value in the **Name** property.

For example, the Name property value for the Combination Chart component of the sample Risk Assessment Status report is Combination Chart1.
5. In OpenPages, go to the reporting fragment field definition and paste or type the value into **Fragment Name**.

For example, for the sample Risk Assessment Status report, you would paste or type Combination Chart1.

Note: If the report prompts for an object or reporting period ID, keep the report open in IBM Cognos Analytics - Reporting.

Obtaining the object ID prompt

Obtain information from IBM Cognos Analytics so you can define **Object ID Prompt** on a reporting fragment field in OpenPages.

Note: This task is required only if a report prompts users to select a resource (such as Entity, Process, and so forth) before running the report. Otherwise, skip this task and leave the field blank.

Procedure

1. In IBM Cognos Analytics - Reporting, open the report:
 - a) On the **Team content** tab, navigate through the folder hierarchy to where the report you want is saved.

For example, Team content > OpenPages Solutions Reports > Risk Assessment Reports > Risk Assessment Status
 - b) Under the Actions column for the report you want, click **Edit report**.
2. For the selected report:
 - a) Click **Pages**.
 - b) Navigate to the prompt page of your report.

3. On the prompt page:
 - a) Click the prompt for the object identifier (such as Entity, Process, and so forth).
 - b) Click **Show Properties** in the application bar.
 - c) Under the **General** heading, click the **Parameter** property icon and copy the value in the box (for example, Entity).

For example, the sample Risk Assessment Status report prompts users to select a Business Entity before running the report. On the sample Risk Assessment Status report PromptPage, you would select the Value Prompt object for Business Entity. The value in the Properties - Value Prompt for the Parameter field is Entity.
4. In OpenPages, go to the reporting fragment field definition and paste or type the value into **Object ID Prompt**.

For example, for the sample Risk Assessment Status report, you would paste or type Entity in the Object ID Prompt box.

Obtaining the reporting period ID prompt

Obtain information from IBM Cognos Analytics so you can define **Reporting Period ID Prompt** on a reporting fragment field in OpenPages.

Note: This task is required **only** if a report prompts users to select a reporting period before running the report. Otherwise, skip this task and leave the field blank.

Procedure

1. In IBM Cognos Analytics - Reporting, open the report:
 - a) On the **Team content** tab, navigate through the folder hierarchy to where the report you want is saved.

For example, Team Content > OpenPages Solutions Reports > Risk Assessment Reports > Risk Assessment Status
 - b) Under the Actions column for the report you want, click **Edit report**.
2. For the selected report:
 - a) Click **Pages**.
 - b) Navigate to the prompt page of your report.
3. On the prompt page:
 - a) Click the prompt for the reporting period identifier.
 - b) In the **Properties** pane, scroll to the **General** heading.
 - c) Under the **General** heading, click the **Parameter** property icon and copy the value in the box.
4. In OpenPages, go to the reporting fragment field definition and paste or type the value into **Reporting Period ID Prompt**.

Creating computed fields

You can create, edit, or view an object field whose value is computed from the values of other fields. These computed fields can exist on either the same object or on another, related object.

About this task

Computed fields have the following characteristics:

- Can be defined in the UI.
- Are always read-only.

- Can be used in reports.
- Can be added to views.
- Must have unique field names. Adding more than one computed field with the same field name in the same view will result in an error.

If you want to import (load) and export (dump) computed field definitions, you must use the ObjectManager tool. For details, see [“Importing computed field definitions” on page 755](#).

Computed fields require an installed and active Cognos server because the fields use the Cognos Computation Handler. If a computed field is executed in the application and the Cognos server is not available, the following message is displayed to users: Cognos is unavailable. Please contact your System Administrator.

Tip: To validate all of the computed fields that are defined for an object type, click  > **Solution Configuration** > **Object Types**, click the object type, and then click **Validate computed fields**.

Procedure

1. In IBM Cognos Analytics - Reporting, model the computed field in a calculation object. For details, see [“Modeling a new computed field in Cognos” on page 182](#).
2. In IBM OpenPages with Watson:
 - a) Define the computed field. For details, see [“Defining a computed field” on page 183](#).
 - b) Regenerate the reporting framework. For details, see [“Updating the reporting framework” on page 817](#).

Modeling a new computed field in Cognos

You can model an equation in Cognos to define a computed field in the application.

Note: If you do not know how to use IBM Cognos Analytics - Reporting, contact an experienced Cognos report author or IBM OpenPages Support.

Procedure

1. Log on to IBM Cognos Analytics as an IBM OpenPages with Watson user with the locale set to **Report Design Language**.
2. Create a list report that you can use to model the computed field equation.
3. Drag the following ID query items onto the report page to establish a context for the calculation:

- An object ID

Example

```
SOXBUSENTITY HIERARCHY >> SOXPROCESS-SOXCONTROLOBJECTIVE HIERARCHY
>> [SOXRISK] >> [RI_RISK_ID]
```

- A reporting period ID

Example

```
SOXBUSENTITY HIERARCHY >> SOXPROCESS-SOXCONTROLOBJECTIVE HIERARCHY
>> [SOXRISK] >> [REPORTING_PERIOD_ID]
```

4. Click **Toolbox** on the **Insertable Objects** pane and complete the following actions:

- a) Drag a **Calculation** object onto the report page.

- b) At the prompt, type a name.

For example, type Calc-Risk.

5. In the **Expression Definition** pane of the model, complete the following actions:

- a) Enter an expression using model query items from the same namespace, function, or parameters.

The Cognos SQL used to define this computed value can be an existing query item in the published Cognos framework or an equation involving multiple query items. Some of the predefined database functions may also be useful for computed fields (such as getting an exchange rate or localizing strings). For details, see the *IBM OpenPages with Watson Report Author's Guide*.

For example, the following equation returns a value with the percentage by which the inherent severity of a risk was reduced after associated controls were applied to that risk. Sample output might be: 2.46.

```
total ([DEFAULT].[SOXCONTROL].[CN_INHERENT_SEVERITY_REDU]
for [DEFAULT].[SOXCONTROL].[RISK_ID]) / 100
```

- b) Validate the expression and make any needed changes.

6. Run the report. Check the results.

7. Click **XML Show Specification** on the toolbar to view the Cognos SQL in an XML representation. The following XML sample shows which sections of the report will be used to define the computed field in IBM OpenPages with Watson and the corresponding field name in the application.

```
<querySet xml:lang="en-ca">
  <BIQuery name="Query1">
    <cube>
      <factList>
        <item refItem="RI_RISK_ID" aggregate="none"/>
        <item refItem="REPORTING_PERIOD_ID" aggregate="none"/>
        <item refItem="Calc-Risk" aggregate="none"/>
      <tabularModel>
        <dataItem name="RI_RISK_ID">
          <expression>[DEFAULT].[SOXRISK].[RI_RISK_ID]</expression>
        </dataItem>
        <dataItem name="REPORTING_PERIOD_ID">
          <expression>[DEFAULT].[SOXRISK].[REPORTING_PERIOD_ID]</expression>
        </dataItem>
        <dataItem name="Calc-Risk">
          <expression>total ([DEFAULT].[SOXCONTROL].[CN_INHERENT_SEVERITY_REDU]
for [DEFAULT].[SOXCONTROL].[RISK_ID]) / 100</expression>
        </dataItem>
      </tabularModel>
    </cube>
  </BIQuery>
</querySet>
```

Note: Because the values in the Report Specification XML window cannot be selected, you can copy the report specification to the Clipboard (**Tools | Copy Report to Clipboard**) and then paste the information into a text document. Then, you can copy the attribute values into the application user interface. The value to be used in the **Equation** definition box can also be obtained from the **Expression Definition** pane of the calculation object.

What to do next

In OpenPages with Watson, define the computed field. For more information, see [“Defining a computed field” on page 183](#).

Defining a computed field

You can define a computed field.

Note: The following data types do not support computed fields: Currency and Enumerated String.

About this task

Once you define a field as a computed field, you cannot undo it.

System Admin Mode must be enabled to do this task.

Procedure

1. Define basic information about the field. For more information, see “[Defining fields and adding them to field groups](#)” on page 161.
2. Select a **Data Type**. For more information, see [Table 88 on page 184](#).

Table 88. Data types for computed fields

Data Type	Return Value	When to Use
Boolean	TRUE or FALSE (case-insensitive)	Takes a Boolean string, parses it, localizes it, and displays it.
Date	Date in the format: yyyy-MM-dd'T'hh:mm:ss	Takes a date string, parses it, localizes it, and displays it.
Decimal	Any numbers	Takes any number string and parses it, localizes it, and displays it.
Integer	Whole numbers	Takes a whole number string and parses it, localizes it, and displays it.
Simple String	Any	Can be used for any computed field. Takes the result of the computation engine and displays it. This will not be localized - it displays the exact output of the computation.

If the field is any other data type, use the Simple String data type.

3. Set **Computed to True**.

When you select **Computed**, the **Required** option disappears and several fields that support computed fields appear.

If you modeled the computed field in IBM Cognos Analytics - Reporting, the values displayed in the **Report Specification XML** window are not selectable (see “[Modeling a new computed field in Cognos](#)” on page 182). You can copy the report specification to the Clipboard (**Tools | Copy Report to Clipboard**), paste the information into a text document, and then copy the attribute values into OpenPages. The value to be used in the application's **Equation** definition box can also be obtained from the **Expression Definition** pane of the calculation object.

4. Enter a value in the **Equation** box. The equation is the Cognos SQL used to define the computed value for the object field. It can be a reference to an existing query item in the published Cognos framework or an equation involving multiple query items.

For example,

```
total ([DEFAULT].[SOXCONTROL].[CN_INHERENT_SEVERITY_REDU] for  
[DEFAULT].[SOXCONTROL].[RISK_ID]) / 100
```

5. Enter a value in the **Primary Namespace** box. The Primary Namespace is the Cognos framework namespace in which the computation is to be performed.

Note: All referenced query items in the values for Equation, Object ID Column, and Reporting Period ID Column must be in the same namespace.

For example, DEFAULT.

6. Enter a value in the **Alternate Namespaces** box if necessary.

The Alternate Namespace is the Cognos framework namespaces to which the computation will be added during reporting framework generation.

Note: See “[Using computed fields with multiple namespaces](#)” on page 185 for an explanation of why a computed field might need alternate namespaces.

7. Enter a value in the **Object Id Column** box. The Object ID Column is a reference to a Cognos framework query item that contains the Resource ID of the computed field's object type. This value must be the same for all computed fields in a given namespace for an object type.

For example: [DEFAULT] . [SOXRISK] . [RI_RISK_ID]

8. Enter a value in the **Reporting Period Id Column** box. The Reporting Period ID Column is the Cognos framework query item that contains the Reporting Period Id of the computed field's object type. This value must be the same for all computed fields in a given namespace for an object type.

Important: The Resource ID and Reporting Period ID must match within the field group and object type. If these values do not match, the validation will fail.

For example, [DEFAULT] . [SOXRISK] . [REPORTING_PERIOD_ID]

9. Enter the package label of the reporting package that the field is run against in **Package Name**.

The value is case-sensitive. The package label for a framework model is defined in the **Platform > Reporting Framework V6 > Models > [model name] > Package Label** setting. If **Package Name** is empty, the package for the Platform Reporting framework model is used.

10. Finish defining the field. For more information, see “[Defining fields and adding them to field groups](#)” on page 161.

Results

The equation is validated against the primary and alternate namespaces.

What to do next

Regenerate the reporting framework to make the computed field available to report authors. For details, see “[Updating the reporting framework](#)” on page 817.

Using computed fields with multiple namespaces

The IBM OpenPages with Watson application allows multiple parent object types for a given child object type.

The Cognos reporting engine cannot support objects with multiple parent's object types.

For example, in the DEFAULT namespace for Operational Risk and Control the only path to a Loss Event is through a Business Entity. This means that if a Loss Event is associated to a parent Risk but not a parent Business Entity, that Loss Event will not be displayed as a result in queries against that namespace. Each parent-child object type relationship that is not contained in DEFAULT is contained in its own namespace.

In order to make the calculation available in multiple namespaces for report writers, you can use the “Additional Namespaces” attribute. This is a comma-delimited list of alternate namespaces for which a “Calculation” object should be created during the framework generation process. During this process, a calculation object is first created for the primary namespace using the value from the “Equation” attribute. Then it creates other calculation objects in other namespaces by taking the equation and substituting the alternate namespaces for the primary namespace.

Note: While an equation might be valid in one namespace, it might not be valid in others. While in most cases this is not a problem, if the query subject name or query item name varies across namespaces, you might need to create separate computed field instances with different equations.

Nesting computed fields

Computed fields can sometimes act as building blocks for other computed fields.

These are referred to as intermediate computations. Currently the IBM OpenPages with Watson application does not support intermediate calculation definitions. If you want to reference another computed field, you must replicate the equation used in that computed field inside the equation for the current field.

For example, if we have a computed field "A" and define it as "A = B × C" and we also know "C = D + E", we would only create one computed field "A" in the application where the equation would be "B × (D + E)".

While this approach can be verbose, it is sometimes the simplest.

Troubleshooting: Computed fields validation

Computed fields validation is complex since they are only valid in relation to the IBM OpenPages with Watson reporting framework, which may change in response to a change in the OpenPages with Watson object model.

Therefore, we provide several forms of validation.

When you create or edit a computed field, the field is validated against the primary namespace as well as all alternate namespaces. If any of the validation checks fail, then the UI will not allow you to save the computed field until the problem is corrected. OpenPages with Watson maintains strict validation checks in this area because a slight error here can have an extensive ripple effect that is hard to identify and correct.

Also, due to the complexity of the computation engine there are certain cases where two computed fields will be valid by themselves but invalid together. A common example is where two computed fields reference different Object ID columns. In order for the computations to be grouped correctly they must all have the same Object ID column value. Therefore, we provide validation functionality across both an entire Field Group definition as well as an Object Type definition.

Troubleshooting: Computed field equation length limitation

Currently there is a limitation on the size of the computation attribute value that can be stored by the application.

The main attribute of concern is Equation where a complex equation could be very lengthy. There is a 20,000 byte limit on the size of the entered text. Note that IBM OpenPages with Watson supports multibyte characters, and so this might not be the equivalent of 20,000 characters if you are using a multibyte language.

Troubleshooting: Computed fields with cross products

A cross product normally occurs when a table of data is joined with itself resulting in redundant data.

In the case of computed fields as they relate to Cognos we encounter a slightly more complex version.

For example, the pre-8.3 ORM solutions schema has computed fields on the Loss Event object type that aggregate associated Loss Impacts and Loss Recoveries. In effect the schema is joining the Loss Event data with itself because the schema has two associations (joins) from the same object type and this causes a cross product.

If you have the following associations between Loss Event and Loss Impact:

- LE - LI1
- LE - LI2
- LE - LI3

And the following associations between Loss Event and Loss Recovery:

- LE - LR1
- LE - LR2

When a query is written to access all three object types the following data is returned:

- LE, LI1, LR1
- LE, LI2, LR1
- LE, LI3, LR1
- LE, LI1, LR2

- LE, LI2, LR2
- LE, LI3, LR2

In the case where we are aggregating values on the Loss Impact, we end up with twice the desired value. And on the Loss Recovery, we get three times the value. One way to work around this is as follows:

Instead of:

```
total (Loss Impacts for Loss Events)
```

Use:

```
average (Loss Impacts for Loss Events) * count (distinct Loss Impacts for Loss Events)
```

Mathematically, we can say that $\text{average} \times \text{distinct_count} = \text{total}/\text{count} \times \text{distinct_count} = \text{total} \times \text{distinct_count}/\text{count}$.

So if we are trying to total the Loss Impacts for a Loss Event in the previous example we would be performing a total on the cross product result and then multiplying by 1/2 to factor out the cross product. If we are trying to total the Loss Recoveries for a Loss Event in the previous example we would be performing a total on the cross product result and then multiplying by 1/3 to factor out the cross product.

Troubleshooting: Optimizing report request performance

With the addition of computed fields there is a large increase in the number of report requests and so it is important to make sure Cognos is set up correctly.

One common pitfall is the number of processes configured for the ReportService. This can be configured as follows.

Procedure

1. From a browser, log on to IBM Cognos Analytics as a user with administrative privileges, for example, OpenPagesAdministrator.

By default, the URL is:

`http://<hostname>/ibmcognos/bi` (if you are using port 80 for Cognos)

Where <hostname> is the name of the Cognos server.

2. Click **Manage > Administration Console** to launch the **IBM Cognos Administration** page.

3. On the **Status** tab, click the **System** link.

4. In the **Scorecard** pane, do the following:

- a) Under **All servers**, click the name of the reporting server you want to tune.

- b) Under the **reporting server**, click the name of the dispatcher. For example,
`http://<server_name>:9300/p2pd`

The dispatcher has the following icon preceding its URI.

- c) In the list of services for the dispatcher, click **ReportService**.

5. In the **Metrics - ReportService** pane, do the following:

- a) Expand **Process**.

- b) View and optionally edit the settings for the **Number of processes high watermark** and **Number of processes low watermark** performance metrics. These metrics monitor the maximum and minimum number of active user sessions since the last reset.

- c) Expand **Queue**.

- d) View and optionally edit the setting for the **Latency** performance metric. This metric specifies the average amount of wait time requests spend in the queue.

- e) Expand **Request**.
- f) View and optionally edit the settings for the **Seconds per successful request** and **Successful requests per minute** performance metrics. These metrics specify the average number of seconds it takes to process a successful request and the average number of successful requests that can be processed in a minute.

6. In the **Settings - ReportService** pane, do the following:

Note: For information on performance metrics and additional settings that are not listed here, see the IBM Cognos Analytics online Help.

- a) Expand **Tuning**.
- b) Change the value of the **Maximum number of processes for the report service during peak period** and **Maximum number of processes for the report service during non-peak period** settings. These settings specify the maximum number of child report service processes that can be started during peak demand and "off-peak" hours.

As a starting point, you should configure the value of these settings to be twice the number of CPUs on the Cognos server. For example, if your environment is always at peak and Cognos is running on a quad-CPU box, then you would set the maximum number of processes to 8 for each setting.

If slow computed fields performance is observed, you can visit the administration page again to observe the number of available processes as well as the latency. Note that these values are only meaningful on a system under load. If all the processes are consistently busy and there is a large latency to service a request, consider changing the number of processes.

Troubleshooting: Computed field query direction performance

While in Cognos it is possible to query up the relationship tree (that is, compute values based on ancestors), but it is strongly discouraged.

When exploring all the computation possibilities there is one large distinction in what can and should be done. The automatic framework generation is set up in such a way as to create joins that are conducive to better performance querying down the relationship tree. A query up the tree will result in bad computed field performance as well as place a large strain on the Database that can result in the entire application slowing down.

Using object fields to launch JavaServer Pages and external URLs

You can customize the OpenPages application to launch JavaServer Pages (JSPs) or external URLs from object fields. You can pass arguments to the JSP or external URL in a URL configuration string that is defined on the object field.

The launchers use simple string fields with a URL display type to show a labeled hyperlink in the application. The URL parameters for the hyperlink can contain system-generated elements, such as the ID of the target object and the current reporting period. The availability of the hyperlink can be controlled by a set of conditions. For example, the link is active when the current user is the Process Owner and they select the current Reporting Period.

The attributes for the launchers are specified by using a URL configuration string that is defined as the default value for the object field, called a URL launcher field in this context. The application processes the configuration string when a view that contains the URL launcher field is rendered. You can add launchers to Creation Views and Task Views. You define the hyperlink's label using application text. You can make the label meaningful for your users. For external URLs, you can make the label a short name that users know rather than a long URL.

To set up a URL launcher field:

1. Define the URL configuration string. Learn about the attributes in the string and study the examples. For information, see ["Attributes in the URL configuration string" on page 189](#) and ["URL configuration string examples" on page 191](#).

2. Define the URL launcher field and add the URL configuration string to it. For information, see “[Adding a URL launcher field](#)” on page 193 .
3. Define the label for the URL launcher field in application text. For information, see “[Configuring application text](#)” on page 192.
4. Add the URL launcher field to profiles and views. For information, see “[Adding a URL launcher field to profiles and views](#)” on page 193.

Attributes in the URL configuration string

The URL configuration string is in JSON format.

It uses the following attributes:

- **labelKey**
- **path**
- **dontPromptForUnsavedChanges**
- **parameters**
- **conditions**
- **popUp**

labelKey attribute

Identifies the application text key for the localized URL text. If it is omitted, the label defaults to **Go**.

path attribute

Specifies the relative path to the target JSP, report, or application object view. If the target is a JSP, then it must be in a folder that is under the sosa application deployment folder. The path attribute is required.

The application root is automatically prepended to the specified path by the application. The application root is determined from the **application.url.path** property in the Server<#>-sosa.properties configuration file.

The path value must contain the leading slash. For example, "path" : "/custom/mycustom.jsp",

dontPromptForUnsavedChanges attribute

By default, dontPromptForUnsavedChanges is set to **false**. Users receive a prompt if they've edited a task view and have not saved their changes. Users must either save or cancel their changes before they can launch the helper.

When dontPromptForUnsavedChanges is set to **true**, the prompt is suppressed. Users can launch the helper without saving their changes. This means that if the helper makes changes to the data, merge conflicts might occur later when the object is saved. Also, if the helper fetches resource data from the server, it will not reflect the unsaved changes.

```
"dontPromptForUnsavedChanges": true
```

parameters attribute

Contains the list of request parameters that are assembled to create the query string of the URL. The parameters are specified as a list of key-value pairs. In most instances, the key names can be anything that you define.

System-populated keys and values are indicated by a \$ in the name. They consist of:

- the ID of the current object, indicated by a parameter value setting of "\$objectId"
- the ID of the current reporting period selection, indicated by a parameter value setting of "\$reportingPeriodId"

Any subset of these parameters can be specified.

Hardcoded parameter values can also be included. For example, where the target JSP or report is reused in different contexts and requires additional information to identify the context for this specific URL launcher field.

The URL parameter values are URL encoded, while the keys are not.

conditions attribute

Defines conditions that must be met in order for the URL to be active.

The conditions can include the following:

- Whether the Reporting Period selected is the current period.
- Whether the target object is locked.
- Whether the value of a specific field matches a value.
- Whether the value of a specific field matches the name of the current user.
- Whether the current user is a member of the group name set in a specific field.

Any subset of the available conditions can be included in the URL configuration string. These conditions are evaluated in the order in which they appear in the string. Each condition can optionally include a `labelKey` that contains an application text string that is displayed when a condition is not met, for example, "Available only for the Process Owner." If the `labelKey` is omitted, the key for the field is applied.

Multiple conditions of the same type can be used, except for the `objectState` and `reportingPeriod` conditions. You can use only one `objectState` and one `reportingPeriod`.

Most errors in the configuration of a condition cause a positive failure in the condition and evaluate to true. The errors are logged. Thorough testing of both positive and negative cases is encouraged to ensure the expected behavior.

reportingPeriod condition

The `reportingPeriod` condition is met when:

- The value of "isCurrent" is true and the user is in the current Reporting Period.
- The value of "isCurrent" is false and the user is in any previous Reporting Period.

objectState condition

The `objectState` condition is met when:

- The value of "isUnlocked" is true and the current object is not locked.
- The value of "isUnlocked" is false and the current object is locked.

fieldValue condition

The `fieldValue` condition evaluates the value of the field against the value that is specified by the `value` attribute by using the specified operator. The target field is identified by using the `FieldGroup.FieldName` convention. The supported operators are "equal" and "notEqual". If the operator is invalid or omitted, the evaluation defaults to "equal".

The Simple String, Boolean, and Enumeration field types are supported. Ensure that you specify the system name and not the localized label for the enumeration values.

The `fieldValue` condition supports checking the current user—by specifying "\$currentUser"—against the value of the target field.

The `fieldValue` condition does not support system fields ("Created by" and "Modified by") or multi actor fields.

popUp attribute

Controls the behavior of the new window. The "windowAttributes" string determines the characteristics, such as size and scroll bars, of the new window that is created when the user clicks the hyperlink. The popUp attribute is optional.

modes attribute (legacy)

Controls whether the URL launcher field is available in edit or view mode.

URL configuration string examples

The following examples illustrate how to define URL configuration strings.

Launching a custom JSP with a popup

The following example launches a custom JSP.

```
$ {
    "labelKey" : "custom.url.labelForMyCustomUrl",
    "path" : "/custom/mycustom.jsp",
    "dontPromptForUnsavedChanges": false
    "parameters" :
    {
        "objId" : "$objectId",
        "repId" : "$reportingPeriodId",
        "isRisk" : "true",
        "includeVersions" : "false"
    },
    "conditions" :
    {
        "reportingPeriod" :
        {
            "isCurrent" : true/false,      // no quotes for Boolean values
            "labelKey" : "custom.url.label.invalid.ReportingPeriod"
        },
        "objectState" :
        {
            "isUnlocked" : true/false,   // note the UN-locked designation
            "labelKey" : "custom.url.label.object.locked"
        },
        "fieldValue" :
        {
            "field" : <"FieldGroup.FieldName">,
            "value" : "$currentUser",
            "operator" : "equal",       // supported operators include "equal" and "notEqual"
            "labelKey" : "custom.url.label.invalid.user"
        },
        "fieldValue" :
        {
            "field" : <"FieldGroup.FieldName">,
            "value" : true,
            "labelKey" : "custom.url.label.invalid.value"
        },
        "fieldValue" :
        {
            "field" : <"FieldGroup.FieldName">,
            "value" : "Undifferentiated",
            "operator" : "notEqual",
            "labelKey" : "custom.url.label.invalid.value"
        }
    },
    "popUp" :
    {
        "windowAttributes" : "height=600,width=800,menubar=no,status=yes,toolbar=no,
scrollbars=yes,resizable=yes"
    }
}
```

Launching a Cognos report

The following example launches a Cognos report from a Command Center redirect with a security condition:

```
 ${{
    "labelKey": "report.name.security.domain.role.assignments",
    "path": "/report.tree.post.do",
    "dontPromptForUnsavedChanges": false
    "parameters": {
        "reportPath": "/_cw_channels/Reporting/SOX/OpenPages Platform Reports/Audit Reports/Security/
Security
Domain Role Assignments.pagespec",
        "label": "Current Reporting Period",
        "entity_id": "$objectId"
    },
    "conditions": {
        "fieldValue": {
            "field": "OPSS-BusEnt.Executive Owner",
            "value": "$currentUser",
            "operator": "equal",
            "labelKey": "custom.url.invalid.user"
        }
    }
}}
```

For this example, you need to add the entity_id parameter to the template that your report is using: CommandCenter Report Redirect or CommandCenter Report Redirect for Cognos Report. For more information, see [“Configuring parameters for Cognos reports” on page 134](#).

Launching a custom JSP

The following example launches a custom JSP.

```
 ${{
    "labelKey" : "url.custom.jsp",
    "path" : "/custom/custom.jsp",
    "dontPromptForUnsavedChanges": false
    "parameters" :
    {
        "Risk Category" : "Damage to Physical Assets",
        "Risk Sub-category" : "Willful Damage"
    }
}}
```

Configuring application text

You can add translated labels for the keys that you specify in the URL configuration string.

Before you begin

To do this task, you need the **SOX > Administration > Application Text** application text.

About this task

For information about application text , see [“Localizing application text” on page 447](#).

Procedure

1. Click  > **System Configuration > Application Text**.
2. Click **New**.
3. Enter the key value in **Name**.
Allowed characters are A-Z, a-z, 0-9, period, underscore, hyphen, and spaces. Special characters are not allowed.
4. Select **Custom** in **Category**.

5. Enter a **Description**. Enter useful information, for example, the URL field that uses the key, in **Description**.
6. Enter the label text in **Default Label**.

If it is displayed, click  to populate translated values to languages. For more information, see “IBM Watson Language Translator” on page 847.

7. In the locale code that you want to modify, for example, French or Japanese, enter text for that language.

If you neither click  nor enter text for each locale code, the text in **Default Label** is populated to all languages.

8. Click **Create**.
9. Repeat these steps for each key in the URL configuration string.

Adding a URL launcher field

The URL launcher field is defined with the URL configuration string as the default value.

Before you begin

Define the URL configuration string before you create the URL launcher field. For more information, see “URL configuration string examples” on page 191.

Procedure

1. Define basic information about the field. For more information, see “Defining fields and adding them to field groups” on page 161.
2. Select Simple String in **Data Type**.
3. Select Link in **Display Type**.
4. Clear the **Required** and **Computed** boxes.
5. Set **Default Value** to the URL configuration string.
6. Finish defining the field. For more information, see “Defining fields and adding them to field groups” on page 161.

Adding a URL launcher field to profiles and views

Add the URL launcher field to profiles and views.

About this task

Add the field to profiles. For more information, see “Including fields in an object type” on page 227.

Add the field to Creation Views and Task Views. The field can display as a button or a link. For more information, see “Displaying a URL launcher field as a button or link” on page 287.

Running the Schema Analysis report

If you already have many fields on an object type, run the Schema Analysis report before you add more fields to the object type. Use the Schema Analysis report to determine the number of object fields that you can add to the object type.

The report shows how many object fields:

- Are currently configured for an object type
- Can “safely” be added to extend that object type

In general, 350 is the threshold limit for the number of fields that can be added to an object type when the average of all field names is 22 characters in length. By keeping the average field name short, it might be possible to include more than the 350 threshold limit for the number of fields.

Important:

Calculations on the Schema Analysis report use and display 175 as the threshold limit rather than 350. You can add more fields than the report shows.

Additionally, each currency field within an object type equates to six fields. This is because each currency field has six distinct columns within the database RT_ table. These six columns equate to the core currency field and its five subfields: Local Amount, Local Currency Code, Exchange Rate, Base Amount, and Base Currency Code.

The Schema Analysis report is accessed through IBM Cognos Analytics. The report lists all object types, in alphabetical order, that are in the schema. The following example shows the name of each column in the report and sample data for the Control object type.

<i>Table 89. Information in the Schema Analysis report</i>	
Report Column Name	Example
Object type	rt_control
Current number of fields	39
Current Field Length Statistics (Highest/Average)	22/14
Number of Additional Fields that can be added (assuming Maximum Field Lengths are used)	136
Potential Number of Additional Fields that can be added (if the Average Field Length for this Object Type does not increase)	187

For example, you want to add three currency fields to the Control object type. Because each currency field equates to six fields, you would be adding 18 fields to the Control object type (3 X 6).

Using the numbers from the Example column in Table 89 on page 194, the Schema Analysis report indicates that the Control object type (rt_control) in the sample schema currently has 39 fields. Of those 39 fields, the largest field length is 22 characters, with an average field length (for all fields) of 14 characters.

The report also indicates that you can add 136 fields with names that do not exceed 22 characters in length, or up to 187 fields if the field names are 14 characters (or less). Adding the three currency fields (for a total of 18 fields) would be well within the threshold for this object type.

The values 136 and 187 are calculated based on 175 as a threshold limit. Since the threshold is 350, you can actually add approximately 311 or 413 fields, respectively.

Procedure

1. Click **Analytics**.
2. Click **Content**.
3. Click **Team content > OpenPages Platform Reports > Administrative Reports**.
4. Click the **Schema Analysis Report** link to run the report.

Chapter 11. Object types

An object type contains metadata about a category of object, such as a Risk or Process object.

From an Object Type page, you can view and access the following information:

- Property information about the object type (such as name, labels, description)
- Field groups, with their field definitions, that are included in this object type
- Allowed parent and child relationships (associations) to other object types
- Filters that are used to narrow the scope of data for this object type
- Dependent fields and pick lists that have been defined for this object type
- Fields for this object type that have been excluded from one or more subsystems

Related information

- Viewing object types in object model diagrams, see [“Solution schema visualizations” on page 195](#).
- Configuring groups, fields, field groups, and filters on object types, see [“Working with object types” on page 198](#).
- Customizing text labels for object types, see [Chapter 18, “Localizing text,” on page 443](#).

Note: If the same management operation is being modified by another administrator, an error message is displayed requesting that you try again later.

Platform object types

The IBM OpenPages with Watson object model is configurable and can contain object types.

Because the object types and schema vary widely from customer to customer, [Table 90 on page 195](#) lists only the Platform object types that are installed, by default, on all systems.

Table 90. Platform object types	
Object Name	Singular Label
SOXBusEntity	Business Entity
SOXIssue	Issue
SOXTask	Issue Action Item
SOXDocument	File
SOXExternalDocument	Link
SOXSignature	Signature

Solution schema visualizations

OpenPages is delivered with system object models that you can view in the solution schema visualization editor. You can also use the editor to create your own solution schema visualizations.

OpenPages is delivered with the following system object models:

- One global object model
- An object model for each OpenPages solution

The solution schema visualization editor is a tool that you can use to view these object models as object model diagrams. In this context, the term *solution* refers to visualizations for object models, be they system object models or solution visualizations that you create.

Using the solution schema visualization editor

Use the solution schema visualization editor to view the OpenPages object models as object model diagrams and create new solution schema visualizations.

To open the solution schema visualization editor, click  > **Solution Configuration** > **Solutions**. Whether the menu item is displayed depends on your access permissions.

Solutions List

The Solutions List shows system object models and user-created solution schema visualizations. From the Solutions List, you can:

- Click a solution. The solution opens in the solution schema visualization editor.
- Click the Name column header to change the sort order of the list.
- Select the checkbox next to a single solution or multiple solutions to update numerous solutions. The bulk update options are:
 - Delete

Clear the check boxes to hide the bulk update options.

System object models cannot be deleted.

- Click  to open a Quick View panel where you can view a list of object types in a solution. For user-created solution schema visualizations, you can also add and remove object types.
- Click **New Solution** to create a new solution schema visualization. After you define the initial properties, the visualization editor opens. For more information, see “[Creating a solution schema visualization](#)” on page 197.

Solution schema visualization editor

Select a solution in the Solutions List and the solution schema visualization editor opens. It has two tabs:

- Map View
- Grid View

Map View

The Map View shows one solution. It has the following components:

- Canvas
 - The canvas shows the object model diagram, including directional arrows that indicate relationships.
 - Click an object type on the canvas and information about the object type displays in the property panel.
 - Move and rearrange the object types.
- Toolbar
 - Icons on the toolbar allow you to control the view on the canvas.

Object Types list panel

The Object Types list panel shows all object types in the solution. It can be displayed or hidden.

- Click an object type in the Object Types panel and it is highlighted in the object model diagram.
- Click  to show an object type that is hidden. Use this icon to control the object types that are displayed on the canvas.
- Property panel

The property panel shows information about a selected object type. It can be accessed from the Map View or the Grid View.

- Expand the **Field Groups** folder to view a list of field groups that are assigned to the object type. Click a field group to view a list of fields that belong to it.
- Expand the **Fields** folder to view a list of fields that are assigned to the object type. Fields are organized by field group.
 - Click  next to a field group to view a list of other object types that use the field group.
 - Click a field name to view it.
- Expand the **Relationships** folder to view a list of parent and child objects types that are associated to the object type.
- Expand the **Profiles** folder to view a list of profiles that are assigned to the object type.
- Expand the **Filters** folder to view a list of filters that are assigned to the object type.
- Expand the **Field Dependencies** folder to view a list of dependent fields that are assigned to the object type.
- Expand the **Dependent Picklists** folder to view a list of dependent picklists that are assigned to the object type.
- Expand the **Views** folder to view a list of views that are assigned to the object type. Click a view to open it in a new tab.
- Expand the **Workflows** folder to view a list of workflows that are assigned to the object type. Click a workflow to open it in a new tab.

The Map View contains the following icons:

Table 91. Icons in the solution schema visualization editor	
Icon	Description
	Changes arrangement based on relationship.
	Resets the zoom.
	Expands (zooms in) the view.
	Shrinks (zoom out) the view.

Grid View

The Grid View shows a list of all object types that belong to a solution.

Click an object type, and it opens in the property panel (see description above).

Click **Show profiles** to display a matrix of object types and profiles that are assigned to them. Select and clear the check boxes to make bulk update changes to profile assignments. If you add a profile, all fields are added. Take care not to clear and re-select profiles because customizations to field assignments are lost and all fields are re-added.

Creating a solution schema visualization

Use the solution schema visualization editor to create new visualizations. For example, you can build visualizations for issue management or loss event management solution schemas.

About this task

A solution schema visualization provides access to object types and relationships.

Procedure

1. Click  > **Solution Configuration** > **Solutions**.
2. Click **New Solution**.
3. Enter an internal **Name** for the solution. It cannot be changed later.
4. Enter a **Description** for the solution.
5. In **Object Types**, assign object types to the solution. Either add them by selecting a profile or add them individually, or both.
6. Click **Create**.

The solution displays in the solution schema visualization editor. For more information, see [“Using the solution schema visualization editor” on page 196](#).

To change the object types that are assigned to the solution after it is created, click  in the Solution List. The Quick View panel opens and you can add and remove object types.

Accessing object types

From an object type, you can configure properties, such as which field groups should be included or excluded, associate parent and/or child object types, manage filters, dependent fields, and so forth.

Before you begin

Log on to IBM OpenPages with Watson as a user with the Object Types application permission set. For more information, see [“Types of application permissions” on page 52](#).

About this task

- When you add a field, you can add it directly to all or a subset of profiles that the object type is assigned to.
- Display Type on fields is defined at the field level on object types.

For more information, see [“Working with object types” on page 198](#).

Procedure

Click  > **Solution Configuration** > **Object Types**.

Working with object types

From an object type, you can add and edit fields, add and edit field groups, add and edit filters, add and edit field dependencies, add and edit dependent picklists, and enable and disable relationships. You can also view profiles, views, and workflows.

Before you begin

Ensure that your user has the **Object Types** application permission.

Procedure

1. Click  > **Solution Configuration** > **Object Types**.
2. Select **Show Profiles** to view all profile assignments on object types. The screen provides a helpful summary of profile assignments per object type. Changes to assignments should be made from profiles because from there you can more clearly view fields and filters and control what the change entails. For more information, see [“Creating a profile” on page 220](#).
3. Click an object type.

4. View information in the **General** section. Values in this section cannot be changed.
5. Expand the **Field Groups** section to add field groups to object types.
For more information, see “[Adding existing field groups to object types](#)” on page 160.
6. Expand the **Fields** section to create and work with fields and field groups.
For more information, see “[Defining fields and adding them to field groups](#)” on page 161.
7. Expand the **Relationships** section. View the parent and child object type associations in the **Parents** and **Children** sections. Select an object type and click **Enable** or **Disable** to change the association. Changes can be made from either the parent or the child object type. For more information, see “[Enabling associations between object types](#)” on page 200 and “[Disabling associations between object types](#)” on page 200.
8. Expand the **Profiles** section to work with profiles.
 - a) Click **Add**.
 - b) Select the box next to each profile to add to the object type.
 - c) Click **Done**.
9. Expand the **Filters** section to work with filters.
To create a filter, see “[Adding filters to object types](#)” on page 208.
To edit a filter, open it, make your changes, and click **Done**.
10. Expand the **Field Dependencies** section to work with dependent fields.
For more information, see “[Adding and working with dependent fields](#)” on page 212.
11. Expand the **Dependent Picklists** section to work with dependent picklists.
For more information, see “[Adding and working with dependent picklists](#)” on page 214.
12. Expand the **Views** section. View the views that are used for the object type.
13. Expand the **Workflows** section. View the workflows that are used for the object type.
14. Click **Validate computed fields** to run validation checks on all of the computed fields that are defined for the object type.

Editing object type properties

You can edit the description of an object type.

Restriction: Do not use characters defined in CJK Unified Ideographs EXTENSION-B on Unicode in the description field.

Before you begin

Ensure that your user has the Object Types application permission.

Procedure

1. Click  > **Solution Configuration** > **Object Types**.
2. Click the name of the object type to modify.
3. Click **Edit**.
4. Make the necessary changes.
5. Click **Done**.

Note: To change label text for an object type, see [Chapter 18, “Localizing text,” on page 443](#).

Disabling associations between object types

If an association between a parent or child object type is no longer needed, disable the relationship between these object types.

For example, if you do not want users to associate certain object types together, such as Accounts with Business Entities, disable the association between the child object type (SOXAccount) and the parent object type (SOXBusEntity).

When you disable an association between object types, the following occurs:

- The child object type is marked as disabled in the **Relationships > Children** section on the parent object.
- The parent object type is marked as disabled in the **Relationships > Parents** section on the child object type.

Before you begin

Ensure that your user has the Object Types application permission.

Procedure

1. Enable System Admin Mode. For more information, see [“Enabling and disabling System Admin Mode” on page 37](#).
2. Click  > **Solution Configuration > Object Types**.
3. From the list, click the name of the object type to modify.
4. Expand the **Relationships** section. Object types are listed in two sections: **Parents** and **Children**.
5. Click the check box next to the object type to disable it.
6. Click **Disable**. The icon in the **Enabled** column changes to an X.
7. To add the object relationship changes to reports, complete the following tasks:
 - a) Update the Reporting Schema. For details, see [“Creating or re-creating the reporting schema” on page 120](#).
 - b) Regenerate the reporting framework. For details, see [“Updating the reporting framework” on page 817](#).

Enabling associations between object types

To allow an association between a parent or child object type that was disabled, enable the association between these object types.

When you enable an association between object types, the following events occur:

- The child object type is marked as enabled in the **Relationships > Children** section on the parent object. The parent object type is marked as enabled in the **Relationships > Parents** section on the child object type.

Before you begin

Ensure that your user has the Object Types application permission.

Procedure

1. Enable System Admin Mode. For more information, see [“Enabling and disabling System Admin Mode” on page 37](#).
2. Click  > **Solution Configuration > Object Types**.
3. From the list, click the name of the object type to modify.
4. Expand the **Relationships** section. Object types are listed in two sections: **Parents** and **Children**.

5. Click the check box next to the object type to enable it.
6. Click **Enable**. The icon in the **Enabled** column changes to a check mark.
7. To add the object relationship changes to reports, complete the following tasks:
 - a) Update the Reporting Schema. For details, see [“Creating or re-creating the reporting schema” on page 120](#).
 - b) Regenerate the reporting framework. For details, see [“Updating the reporting framework” on page 817](#).

Configuring OpenPages to associate a large number of child objects

If the number of associations that you add exceeds the maximum, the result is a long running process. The default maximum is 250. This information applies only to child associations, not parent associations.

About this task

You can use IBM OpenPages with Watson to associate a large number of child objects to a parent object. When the number of child associations exceeds the limit set in the **Max Child Associations Interactive** setting, the process runs in the background and you receive an email when it completes.



Trouble: If you are using Oracle, you might see an error such as OP-00700- The requested operation could not be completed and see ORA-01795: maximum number of expressions in a list is 1000 in the log. This Oracle error can happen when you're associating many objects, for example.

These settings are set by default. You can change the following settings to specify the maximum number of associations, the timeout length, and the email response to a long running process.

Procedure

1. Click > **System Configuration** > **Settings**.
2. To specify the number of child objects to associate before background processing begins:
Applications > **Common** > **Configuration** > **Max Child Associations Interactive**. The default is 250.
3. To specify the transaction timeout for the background process, click **Platform** > **Processes** > **Associate Resources** > **Transaction Timeout**. The default is 21600 seconds.
 To show the **Transaction Timeout** setting, change the value of **Applications** > **Common** > **Configuration** > **Show Hidden Settings** from false to true. The default value is false.
4. To specify the email settings for the email server configuration, click:
 - **Applications** > **Common** > **Email** > **Mail Server**
 - **Applications** > **Common** > **Email** > **SMTP Password**
 - **Applications** > **Common** > **Email** > **SMTP Port**
 - **Applications** > **Common** > **Email** > **SMTP Security Type**
 - **Applications** > **Common** > **Email** > **SMTP User Name**
5. Optional: You can customize the email subject and content. Click > **System Configuration** > **Application Text**, and then use the following strings:
 - **com.resource.association.email.subject.success**
 - **com.resource.association.email.subject.warning**
 - **com.resource.association.email.subject.error**
 - **com.resource.association.email.content.success**
 - **com.resource.association.email.content.warning**

Limiting parent and child relationships

You can limit a user to selecting only one parent of a specified object type for a given child object type.

Before you begin

Ensure that you have the Object Types application permission.

Procedure

1. Enable System Admin Mode. For more information, see [“Enabling and disabling System Admin Mode” on page 37](#).
2. Click  > **Solution Configuration** > **Object Types**.
3. From the list, click the name of the child object type whose parent relationships you want to limit.
4. Expand the **Relationships** section.
For each object type in the **Parents** section, the **Single parent max** column displays an **X** if the number of parents is not limited.
5. From the list, select the check box for the parent object type to limit.
6. Click **Set single parent max**.

Results

The **Set single parent max** column displays a checkmark.

To remove the limit, select the check box for the parent object type, and then click **Remove single parent max**.

If you're working with a recursive object type, selecting **Remove single parent max** does not permit multiple parents of the same type as the recursive object. A recursive object can have only one parent of its same object type.

A *recursive object type* can have a parent object and child objects of its own type, potentially multiple layers deep. Examples of recursive object types include business entities, sub-accounts, sub-mandates, and sub-processes. For example, a business entity can have a parent business entity, such as Global Financial Services, and multiple child business entities, such as Compliance, Finance, HR, and IT, each of which can have child business entities.

Example

For example, if you want to limit Accounts to having only one Audit parent each, perform the following steps:

1. Click  > **Solution Configuration** > **Object Types**.
2. From the list, click **Account**.
3. Expand the **Relationships** section.
4. Select the **Audit** check box.
5. Click **Set single parent max**.

Configuring file types for file attachments

Configure the types of files that can be uploaded as file attachments and, optionally, included in global search. File types are configured only for the File (SOXDocument) object type.

A file type describes the structure or format of a file and is typically reflected in the file name extension.

Some common examples of file name extensions include .rtf (Rich Text Format), .txt (ASCII text), .docx (Microsoft Word), .pdf (Portable Document Format), .xlsx (Microsoft Excel), .htm (Hypertext Markup Language), and .jsp (Java Server Page).

In IBM OpenPages with Watson file type extensions are case sensitive. When you attach a file to an object, the file extension is case-sensitive and must match the extension specified in the **File Types Information** section of the SOXDocument object type.

Each file type has a corresponding MIME (Multipurpose Internet Mail Extension) type associated with it, which is a standardized data exchange method used by Web browsers to associate files with helper applications that display files of that type. For example, a MIME type of image/gif, informs the browser to handle the data as an image. The IBM OpenPages with Watson application supplies a number of predefined MIME types.

Adding a file type

When you add a file type to the application, it is automatically added to the File Type Information selection list.

Before you begin

Ensure that your user has the Object Types application permission.

Procedure

1. Click  > **Solution Configuration** > **Object Types**.
2. Click the **File** object type.
3. Expand the **File Types Information** section.
4. Click **Show Disabled Types** to verify that the type you want to add does not already exist.
5. Click **New File Type**.
6. Enter a **File Extension**. Use the correct case because file type extensions are case-sensitive.
7. Enter a **MIME Type**, for example, image/cgm, that corresponds to the file extension.
8. Click **Create**.

What to do next

Enable the new file type. For more information, see [“Enabling and disabling file types” on page 203](#).

Enabling and disabling file types

You can enable and disable file types for the File (SOXDocument) object type.

Before you begin

Ensure that your user has the **Object Types** application permission.

Procedure

1. Click  > **Solution Configuration** > **Object Types**.
2. Click the **File** object type.
3. Expand the **File Types Information** section.
4. Select a file type with the check mark.
5. Select **Enable**.

Results

Users can add file attachments of the enabled file type to objects.

File types cannot be deleted, they can only be disabled. Repeat the steps and select **Disable** to disable a file type. Click **Show Disabled Types** to view all file types.

Enabling and disabling global search for file types

You can enable and disable global search for file types for the File (SOXDocument) object type.

Before you begin

Ensure that your user has the Object Types application permission.

About this task

Do not enable global search for file types that are binary, or that are media such as images, audio, and video. Global search ignores these file types, even if enabled.

Procedure

1. Click  > **Solution Configuration** > **Object Types**.
2. Click the **File** object type.
3. Expand the **File Types Information** section.
4. Select a file type with the check mark.
5. Select **Enable Global Search**.

Results

The content of file attachments of the file type are included in global search results.

Repeat the steps and select **Disable Global Search** to disable global search for a file type.

Note: Files might still be discovered after the file type is disabled for global search. If a file extension is associated with more than one MIME type, then files with this extension are still discovered until all associated MIME types are excluded or are disabled from search. Disable each associated MIME type to remove the types from searches.

What to do next

Update global search to include the file type. For more information, see [“Enabling attachment file types for global search” on page 522](#).

Configuring filters for an object type

Filters are specific to an object type and are used to narrow the scope of data that is returned in a view for that object type.

When you create a filter for an object type, you can select which fields to use to search for data. Only the objects that match the specified search criteria are returned for that object type.

Filters that are created by administrators are also called public filters. Public filters are usable by any user who has them in their profile. Users can also create their own private filters.

Filters are used in views, workflows, dashboard panels, charts, and more.

The following table provides an overview of the flow of tasks for adding filters to object types and views.

Table 92. Tasks for configuring filters and views		
Task	Task Description	Related Topic
1	Determine the purpose and characteristics of the filter.	“Filter considerations” on page 205

Table 92. Tasks for configuring filters and views (continued)

Task	Task Description	Related Topic
2	Add the filter to an object type.	“Adding filters to object types” on page 208
3	Add localized names for the filter (optional)	“Modifying object text ” on page 445
3	Apply the filter in various places, for example, views.	

Filter considerations

Before you create a filter, determine the characteristics of the filter and identify the object type on which the new filter is used.

For instructions on creating a filter, see [“Adding filters to object types” on page 208](#).

The following list identifies information that you need before you create a new filter:

- Object type - Which object type will the filter be used with?
- Name - How will the new filter be identified? The name of the filter is important because it is also the initial label that will appear for the filter in the application.
- Profiles - Which profiles will be associated with the filter?
- Filtering criteria - Which fields are used in the filter criteria to narrow the scope of data returned by the search?
- Views, dashboard panels, and more - Where is the filter needed?
- Localization - Does the filter name need to be localized? If so, the translated names are defined by using object text. For more information, see [“Modifying object text ” on page 445](#).

Example

You create a filter for risk assessments called "In Progress" that displays all risk assessments due within the next three months, and has the following selected fields and values:

Table 93. Sample risk assessments fields

Field	Value
Status	In Progress
Start Date	On this date
End Date	In the next 90 days

If you associate this filter to the "Assessors" profile, application users who are assigned the Assessors profile would then be able to select this filter in various places. For example, if they create a dashboard panel, chart, or Grid View for the Risk Assessment object type, they can apply the filter.

Limitations on special characters in filters for long string fields

When you create filters for long string fields, some special characters have limitations on how they are used.

Do not use special characters as first or last character

When you use a filter to search for text in long string fields, the following special characters and symbols might not return the expected results if these characters are the first or last character in the text to be searched:

- Characters in languages such as Chinese, Japanese, and Thai.

- Some three-byte Unicode characters and symbols such as * № € Å ☆ @

Note: When you search for text that contains these special characters, you must use the **Contains** search condition in the filter.

For example, you want to search for text that has the phrase "maximum € 120". For the selected text field, you would choose the **Contains** search condition, and type the words: maximum € 120.

The search results would return the following: "The maximum € 120 is the upper limit" because the special character appears in the middle of the text and not at either the beginning or end.

The search results would NOT include the following: "€ 120 is the maximum upper limit" or "The maximum upper limit is 120 €" because the special character is the first or last character in the text.

Important: You can use the forward slash to create filters for folders. If you want to start or end your filter with a forward slash, then you must use a double forward slash. The first forward slash is stripped out. For example, if you enter a folder, enter it as //foldername.

Reserved characters

Table 94. Reserved characters that have special meaning in the filters

Reserved character	Description
_	An underscore is used as a single character wildcard.
%	A percent sign is used as a multiple character wildcard.

Do not use these special characters

The following special characters are not validated.

Table 95. Special characters that are not supported in search filters

Special Character	Description
&	Ampersand
@	At symbol on keyboard
!	Exclamation point or bang
\	Backward slash
^	Caret or circumflex
:	Colon
;	Semicolon
,	Comma
-	Dash
>	Greater than sign
<	Less than sign
(Opening parenthesis
)	Closing parenthesis
=	Equal sign
	Pipe or vertical bar

Table 95. Special characters that are not supported in search filters (continued)

Special Character	Description
+	Plus sign
#	Pound or number sign, hash symbol
?	Question mark
~	Tilde or equivalency sign
`	Grave accent
[Opening bracket
]	Closing bracket
{	Opening brace
}	Closing brace
\$	Dollar sign
¥	Yen sign
₩	Won sign
ᠤ	Yi syllable IT
	Double vertical lines

The following reserved words are not supported in the search filter and should not be used:

- ABOUT
- ACCUM
- AND
- BT
- BTG
- BTI
- EQUIV
- FUZZY
- HASPATH
- INPATH
- MDATA
- MINUS
- NEAR
- NOT
- NT
- NTG
- NTI
- NTP
- OR
- PT
- RT

- SQE
- SYN
- TR
- TRSYN
- TT
- WITHIN

Note: Reserved words are not case-sensitive.

Adding filters to object types

Filters are specific to an object type and narrow the scope of data that is returned in a view for the object type. When you create a filter for an object type, select which fields to use to search for data. Only the objects that match the specified search criteria will be returned for that object type.

For up-to-date results of filters that include long string fields, the text index for the long string field must have been synchronized with the values in the field. Synchronization depends on when the index was created or the setting of scheduled synchronization. For details on the index creation and synchronization utilities provided for long string filtering, see “[Utilities for filtering on long string field content in a Db2 database](#)” on page 566 or “[Utilities for filtering on long string field content in an Oracle database](#)” on page 610.

Note: If you create a new filter that uses the character % as the value, for example Name Contains %2, the Name Contains value field appears empty after you load the filter: the % character does not appear. However, the filter runs properly.

Before you begin

Log on with a user that has the Object Types application permission.

Procedure

1. Click  > **Solution Configuration** > **Object Types**.
2. Click an object type.
3. Expand the **Filters** section to work with public filters.
4. Click **New Filter**.
5. Enter a **Name**.
6. Enter a **Description**.
7. Click **New Condition** to define a condition.
 - a) Select a **Field**.
 - b) Select an **Operation**. The available operations and remaining fields depend on the field you selected.
 - c) Complete the remaining fields.

For example, for a name field, the options are **Starts with**, **Ends with**, **Contains**, and **Equals** and a text value.

Note: Text is not case-sensitive.

Table 96. Search conditions

If a condition field is a	You can do this
A user	Select the Matches the selected user operation and add one or more users in the list under Other user . Or, you can set End User to resolve to the currently logged-on user.

Table 96. Search conditions (continued)

If a condition field is a	You can do this
A group	Select the Includes all of the selected users operation and add one or more groups in the list under Other group . Or, you can set End User to resolve to the currently logged-on user.
An enumerated value	Select the Any of the following values operation and add enumerated values in the list under Select Values . You can also set Show hidden values .
A string value	Select an operation (such as Starts with , Contains , Equals , and Ends with) and then enter a value.
A date	Select an operation (such as In the last , In the next , On a specific date , and In the range) and then enter a value.
A numeric value	Select an operation (such as Equals , Greater than , Less than , and In the range) and then enter a value.
A Boolean	Click true or false .

Important: For limitations on the special characters in filters for long string fields, see “[Limitations on special characters in filters for long string fields](#)” on page 205.

- d) Click **Done**.
- e) Optional: Add more conditions.
- f) Optional: Set **Advanced Logic** to true to override the default rule that all conditions must be met. Write a statement in **Logic**. Use the condition numbers together with the operators and, or, not, and parentheses.

The order of operations is: () then NOT then AND then OR.

For example:

- 1 or 2 or 3
- 1 and (2 or 3)
- 1 not (2 or 3)

For details on specifying more complex logic for your filters, see “[Using advanced logic in a search filter](#)” on page 210.

8. Expand **Profiles** and assign the filter to one or more profiles.

Although a profile is not required, a filter must be assigned to a profile to be available to use.

9. Click **Done**.

What to do next

If the filter name must be localized, see “[Modifying object text](#)” on page 445.

Using advanced logic in a search filter

You can add advanced logic to filters to help refine searches using logical operators such as OR, NOT, and parentheses. By default, the system uses only the AND operator to return results from a filtered search. Advanced logic is also referred to as complex logic.

When you create a filter (see “[Adding filters to object types](#)” on page 208) you select object fields and define the search criteria for each selected field. These key fields are then used by the system to search the database for objects that meet the specified criteria.

Every key field that is selected in a filter is displayed in a row that is sequentially numbered. This number of the row is its identifier. For example, the first key search field is displayed in row number 1, the next key search field is in row number 2, the next one in row number 3, and so forth. You use the row identifier with a logical operator to create an advanced logic search expression. Although row identifiers are sequential, the identifier can appear in any order within the expression.

Use the logical operators described in the following table to define filtered searches. The operators are not case-sensitive.

Table 97. Logical operators for advanced logic		
Operator	Purpose	Example
AND	Narrow the search for objects that meet all the search criteria. This is the default operator used to return results from a search filter.	1 AND 2 AND 3
OR	Broaden the search for objects that meet one or the other key search criteria.	1 OR 2 OR 3
NOT	Narrow the search for objects by excluding the specified key search criteria.	1 AND NOT 2
()	Group search criteria together to show the order in which the query should be applied.	1 AND (2 OR 3)

Procedure

1. Create or access a filter. For more information, see [“Adding filters to object types” on page 208](#).
2. Expand the **Filters** section to work with public filters.
3. Add conditions.
4. In a **Filter** window (adding or editing a filter), set **Advanced Logic** to true.
5. In the **Logic** text box, enter a search expression using conditions and logical operators.
6. Click **Done**.

Examples

- You have 3 search fields defined in your filter. By default, the system uses only the AND operator so it would retrieve objects that only matched all 3 fields (1 AND 2 AND 3). If, however, you wanted to broaden the search so it included field 1 and either fields 2 or 3, use the OR operator to modify the search to retrieve all objects that matched field 1 and matched either fields 2 or 3.

To do this, create the logical expression: 1 AND (2 OR 3).

- You want to find open Issue objects that are not assigned to you. To create such a filter, you would select the “Issue Status” field and choose the “Open” value (this is field 1). Then select the “Assignee” field and choose your name from the **Select the user** window or click the **End User** link (this is field 2).

To exclude your name from the search results, in the **Logic** text box, you would type 1 AND NOT 2.

Note: The NOT operator does not return objects that have an empty, blank, or null value in the selected field criteria. This means that any unassigned Issue objects (that is, the "Assignee" field was empty or blank), would be excluded from the search results.

Configuring dependent fields

You can configure a field so that its behavior - Visible, Editable, or Required - is dependent upon some value selected by a user in another field or set of fields.

A dependent field can have multiple behaviors and controlling fields. When you add a dependent field, configure the field and a behavior. Then, select the field and value that control the behavior.

If you want a dependent field to have multiple behaviors, such as Required and Visible, configure the field separately for each behavior.



Attention: If you configure a field to be required, it is still required even if it is not visible. This ability is for cases where the hidden field is updated by a separate activity, but the field is still required.

If you have multiple controlling fields for a specific behavior, you configure what conditions must be met before the behavior of the dependent field is triggered. The conditions are identified in the following list:

- Dependent fields cannot include System Fields.
- Controller fields must be enumerated string lists (single or multi-selectable) or Actor fields (User Selector, Group Selector, User/Group Selector, Multi User Selector, Multi Group Selector, or Multi User/Group Selector). If you configure a controller field with multiple values that are combined with an AND, all controller values or criteria must match. If you configure a controller field with multiple values that are combined with an OR, only one of the controller values or criteria must match. When the values or criteria match, the dependent field behavior is triggered.
- Computed fields and report fragment fields can have only a behavior of Visible.

Important: If a field level security rule is applied to the controlling field, field dependencies that use the controlling field can no longer function as expected. The security restrictions that are built into the field level security rule apply to actions throughout the system and, therefore, prevent the field dependency from being evaluated. For more information, see ["Field level security" on page 92](#).

In the UI:

- Dependent field behavior is applied in Grid Views, Task Views, Creation Views, and Quick Views.
- In Grid Views, if a dependent field column is shown, the column values adhere to the field dependency behavior.

Example

You want to know who performs a control activity if a user selects No to the question **Does the Control Owner perform the Control?**.

You could configure the behavior of the field **Does the Control Owner perform the Control?** to be dynamic so that the field is both visible and required only if the user selects No to the question **Does the Control Owner perform the Control?**. If the user selects Yes, then this field would remain hidden from the user.

The **Does the Control Owner perform the Control?** field is considered the *dependent* field as the behaviors of this field (Required and Visible) depend on the value (No) selected in the *controller* field, **Does the Control Owner perform the Control?**.

Adding and working with dependent fields

The dynamic behavior of dependent fields can be used to help guide users during the creation or editing of an object.

Before you begin

Log on with a user that has the Object Types application permission.

About this task

For more information about dependent fields, see [“Configuring dependent fields ” on page 211](#).

Field dependencies can be enabled, disabled, copied, modified, and deleted.

When a dependent field is disabled, the application does not enforce the conditions that control the behavior of the dependent field.

If you have multiple field dependencies that use the same controller conditions, click **Copy Controllers to New** to quickly duplicate existing controller conditions to the same or different dependent fields within the same object type.

After you create a dependent field, you can add, remove, or modify the fields that control the behavior of the dependent field. In the case of multiple controllers, you can also change the operator that determines whether one or all the controller conditions must be met before the dependent field behavior is triggered.

When deleting field dependencies, if a dependent field is also used as a controller in other dependencies, you must first remove the dependencies on that field before deleting it. If you want to keep a dependent field but do not want its behavior, you can disable it rather than deleting it.

If you create field dependencies and dependent picklists that create a loop, an error is displayed in the interface that states that "The operation is not allowed because it would result in the following circular dependencies ...". If you are upgrading and you had a loop in the previous version, if you change your configuration you will get an error in the interface that states that "The operation is not allowed because it would result in the following circular dependencies ...".

Procedure

1. Click  > **Solution Configuration** > **Object Types**.
2. Click an object type.
3. Expand the **Field Dependencies** section.
4. Click **New Dependency**.
5. From the **Dependent Field**, select a field from the list.
6. In **Behavior Type**, select one of the following values:

Table 98. Behavior Type values

Value	Description
Required	Require the user to enter a value in the dependent field only if the controlling field is selected.  Attention: If you configure a field as required, it is required even if it is not visible. This ability is for cases where the hidden field is updated by a separate activity, but the field is still required.
Editable	Enable the user to modify this dependent field only if the controlling field is selected. Otherwise, the dependent field is read only.

Table 98. Behavior Type values (continued)

Value	Description
Visible	Display the dependent field to the user only if the controlling field is selected. Otherwise, the dependent field are hidden from view.

7. Select a value in **Controlling Field Logic**:

Table 99. Controlling Field Logic

Select this value	If you want
And	All the selected controller fields to be used to meet the condition. This is the default operator value.
Or	Only one of the selected controllers to be used to meet the condition.

8. Click **Add** in **Controlling Fields**.

- a) Choose a field in **Controlling Field**.
- b) In the **Controlling Values** box, select one or more values from the list and click **Add**.
- c) Set **End User** to true or false, if displayed. It compares the field to the signed on user.
- d) Click **Create**.
- e) Add more controlling fields, as needed.

9. Click **Create**.

The newly created field dependency is listed on the **Field Dependencies** pane.

Configuration settings for creating new objects

Creation Views provide a way for users to easily add new object instances. Some of the configuration settings for creating new objects apply globally and some are profile and object type specific.

For information about how to create new object instances, see [“Creation Views” on page 250](#).

For most object types, you can auto-generate their names when they are created. This allows users to enforce internal naming policies and ensure unique object names. You can turn auto-naming on or off for each object type individually. For information on how to specify the Auto-naming feature, see [“Object auto-naming settings” on page 483](#).

Controlling the availability of object types with the New button on Grid Views

You can configure which object types cannot be created from  on Grid Views. This setting takes effect for all users and all profiles.

About this task

From a Grid View, the parent object is not prepopulated like it is in relationship fields. Restricting the parent object selection can help and supports users to do a better job of selecting correct parent objects.

Procedure

1. Click  > **System Configuration** > **Settings**.
2. Navigate to **Applications** > **GRCM** > **Add New Wizard**.
3. Click **Object Types Disabled**.

4. In the **Value** box, type the names of the objects that you want to disable. Separate each object type with a comma (,). Be sure to use the object names and not the object labels.
5. Click **Done**.

Configuring dependent picklists

You can configure a list of items so that the items in the list are filtered based upon some value selected by a user in another list.

The filtering of lists can be used to help guide users in the selection of relevant values from lists during the creation or editing of an object.

Example

Both the Risk Category and Risk Subcategory fields of a Risk object (SOXRisk) have many items in their respective lists from which a user can choose, and you want only the values of "Theft and Fraud" and "Security Systems" to be displayed in the Risk Subcategory list when a user selects "External Fraud" from the Risk Category list.

To filter the list, you would map the Risk Subcategory values of "Theft and Fraud" and "Security Systems" to the Risk Category value of "External Fraud".

The Risk Subcategory field with its selected values is considered the *dependent picklist* as the behavior of this list depends upon the value selected in the Risk Category field or *controller picklist*.

Adding and working with dependent picklists

When you create a dependent picklist, you map one or more dependent field list values to one or more controlling field list values.

Before you begin

Log on with a user that has the Object Types application permission.

About this task

For more information about dependent picklists, see ["Configuring dependent picklists" on page 214](#).

Dependent picklists can be enabled, disabled, modified, and deleted.

By default, dependent picklists are enabled when created. When a dependent picklist is disabled, the application does not enforce the conditions of the picklist.

After you create a dependent picklist, you can modify the values that are displayed in the dependent picklist.

When you delete a dependent picklist, it is permanently removed and cannot be restored. If you want to keep a dependent picklist but do not want to enforce it, you can disable it rather than deleting it.

If you create field dependencies and dependent picklists that create a loop, an error is displayed in the interface that states that "The operation is not allowed because it would result in the following circular dependencies ...". If you are upgrading and you had a loop in the previous version, if you change your configuration you will get an error in the interface that states that "The operation is not allowed because it would result in the following circular dependencies ...".



Attention: When using the bulk update feature, the dependent picklists do not change values when the controlling value changes. Instead, all values from both the controller and the dependent picklist are displayed. Validation of selected values is done before the objects are saved and conflicts are reported back to the user.

Procedure

1. Click  > **Solution Configuration** > **Object Types**.
2. Click an object type.
3. Expand the **Dependent Picklists** section.
4. Click **New Dependency**.
5. From the **Dependent Field**, select a field from the list.
6. Click **Add in Controlling Fields**.
 - a) Choose a field in **Controlling Field**.
 - b) Under **Controller values**, expand a value.
 - c) Click **Add** next to **Dependent Values**.
 - d) Select the values that you want to map.
 - e) Click **Create**.
 - f) Map more values, as needed.
7. Click **Create**.

The newly created dependent list is listed on the **Dependent Picklists** section.

Example

The following example shows how Risk Category, the *controlling field*, and Risk Subcategory, the *dependent field*, are mapped on Risk object (SOXRisk) type.

Each controller value group contains values in the controlling picklist (Risk Category in this example) that are mapped to values in the dependent picklist (Risk Subcategory in this example).

The Risk Subcategory values "Theft and Fraud" and "Unauthorized Activity" are selected for Internal Fraud. "Theft and Fraud" and "System Security" are selected for External Fraud. If a user selects "Internal Fraud" as the Risk Category, only "Theft and Fraud" and "Unauthorized Activity" values will be displayed on the Risk Subcategory list. Similarly, if a user selects "External Fraud" as the Risk Category, only the "Theft and Fraud" and "Systems Security" values will be displayed in the Risk Subcategory list.

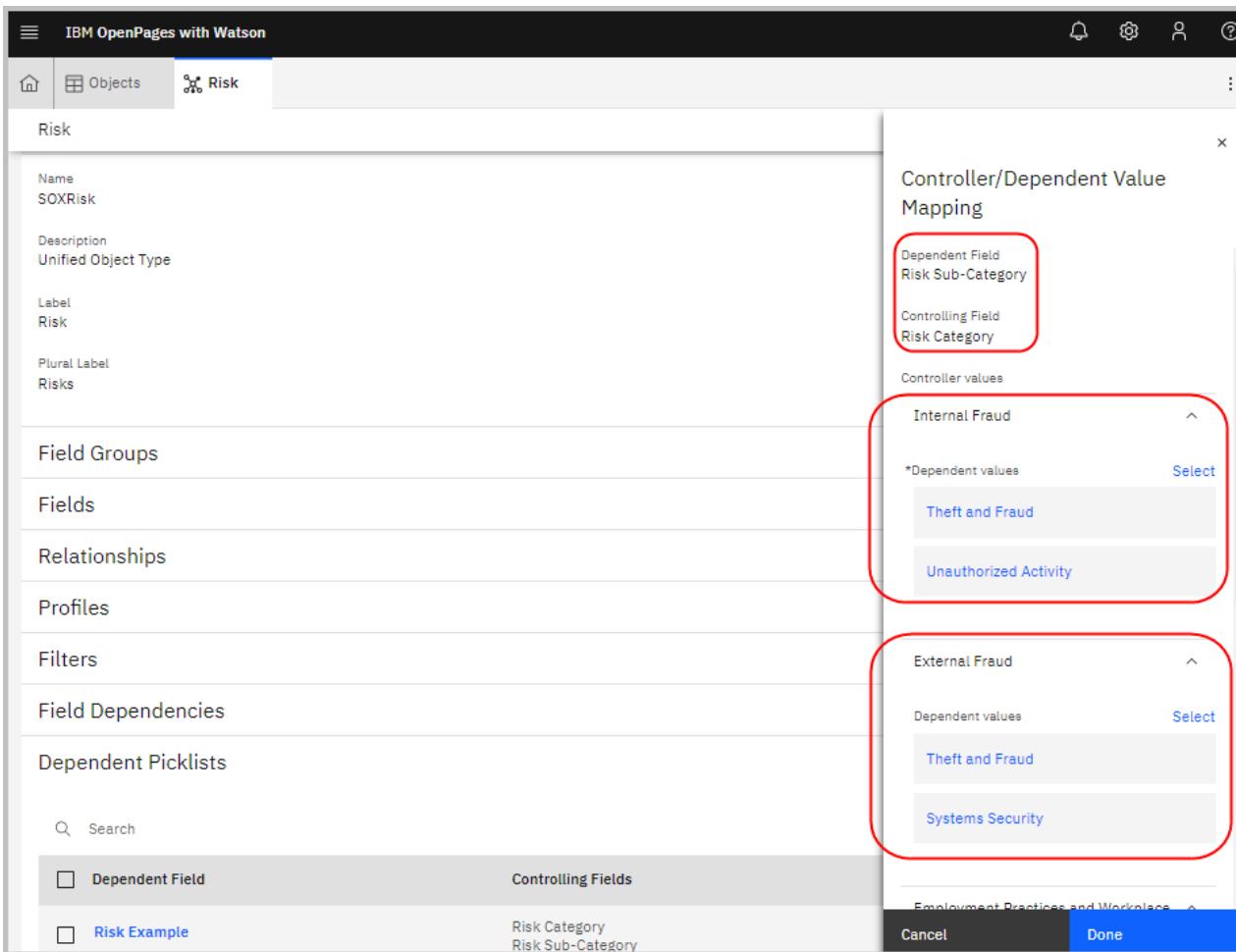


Figure 13. Sample picklist mapping

Excluding fields from a subsystem

IBM OpenPages with Watson contains multiple subsystems or components that comprise a larger software system.

These subsystems (for example, Reporting Schema and Reporting Framework), typically use field definitions. In some situations, a field that is applicable to one subsystem may not be applicable to another.

For example, suppose that you want to streamline the number of fields that are used for generating Test (SOXTest) object reports. You are not required, for example, to produce a report on Testing Steps, a field that is part of the Test object. You could exclude the Testing Steps field from the Reporting Schema and the Reporting Framework subsystems. When you regenerate the reporting schema and the framework, the Testing Steps field is ignored and is excluded from the schema and framework.

Selecting the fields to exclude

When you exclude a field from a subsystem, the subsystem ignores the excluded field.

The following table identifies that action that occurs when selected fields are excluded:

Table 100. Field exclusions and results

Fields excluded from this subsystem	Results
Reporting Schema	<p>Any application components that use the field need to be updated to remove references to the excluded field. For example, you might need to update security rules, reports, and views.</p> <p>If you exclude a field from the reporting schema, also exclude it from the reporting framework. If you use global search, also remove the field from global search. For more information, see “Enabling or disabling object types or fields for global search” on page 523.</p> <p>Note: A field that is excluded from the reporting schema must also be excluded from global search. If you want to use global search on a field, do not exclude it from the reporting schema.</p> <p>Note: When you use the IBM OpenPages REST API, a select * statement returns all fields except the fields that are excluded from the reporting schema. For more information, see the <i>IBM OpenPages with Watson GRC REST API Guide</i>.</p>
Reporting Framework	Any reports (existing or future) that reference these fields fail unless the excluded field is also removed from the report.

Before you begin

To do this task you need the **Object Types** application permission.

Procedure

1. Click  > **Solution Configuration** > **Object Types**.
2. From the list, click the name of the object type to modify.
3. Expand the **Field Exclusions** section.
4. Click **Exclude**.
5. Complete the following fields in the **Exclude** panel:
 - a) In the **Name** field, select the fields that you want to exclude from the subsystem.
 - b) In the **Subsystem** field, select the subsystem.
6. Click **Create**.
7. To exclude fields from a different object type, repeat Steps 1 - 6.
8. If you excluded fields from the Reporting Schema subsystem, re-create the reporting schema.
For more information, see [“Creating or re-creating the reporting schema” on page 120](#).
9. If you excluded fields from the Reporting Schema or from the Reporting Framework subsystem, regenerate the reporting framework.
For more information, see [“Updating the reporting framework” on page 817](#).

Changing the subsystem for an excluded field

You can change the subsystem for individual fields that have been excluded from a subsystem.

Before you begin

To do this task you need the **Object Types** application permission.

Procedure

1. Click  > **Solution Configuration** > **Object Types**.
2. Select the name of the object type you want to modify.
3. Expand the **Field Exclusions** section.
4. Click the name of a field.
5. In **Subsystem**, modify the subsystem.
6. Click **Done**.
7. If you modified the list of fields that are excluded from the Reporting Schema subsystem, re-create the reporting schema.
For more information, see “[Creating or re-creating the reporting schema](#)” on page 120.
You must re-create the reporting schema for the changes to take effect.
8. If you modified the list of fields that are excluded from the Reporting Schema or from the Reporting Framework subsystem, update the reporting framework.
For more information, see “[Updating the reporting framework](#)” on page 817.

Removing excluded fields

You can remove a field from the list of excluded fields.

When you remove a field from the list of excluded fields, the field is removed from the **Field Exclusions** section for the object type.

Before you begin

To do this task you need the **Object Types** application permission.

Procedure

1. Click  > **Solution Configuration** > **Object Types**.
2. From the list, click the name of the object type you want to modify.
3. Expand the **Field Exclusions** section.
4. Select the check box next to the excluded field you want to remove. You can select multiple boxes.
5. Click **Delete**.
6. Click **Delete** again to confirm.
7. If you modified the list of fields that are excluded from the Reporting Schema subsystem, re-create the reporting schema.
For more information, see “[Creating or re-creating the reporting schema](#)” on page 120.
You must re-create the reporting schema for the changes to take effect.
8. If you modified the list of fields that are excluded from the Reporting Schema or from the Reporting Framework subsystem, update the reporting framework.
For more information, see “[Updating the reporting framework](#)” on page 817.

Chapter 12. Profiles

Profiles provide end users with a localized view of information that is directly related to their responsibilities.

Use profiles to configure objects, fields, and object views. When you change a setting in a profile, the change is dynamic and the change is immediate. Reports can be added to profiles.

Each user has one or more profiles available to them for their logon session.

You can use profiles to restrict the object types that individual users can view. You can also define the fields in each object that are visible to them. If an object type is absent from a profile, that object type is hidden from users of that profile. You can also assign reports to a profile.

Create profiles by cloning them from existing profiles, then modifying the new profile. A standard profile, called Default, is provided. You can use it as a template to create other profiles. The profiles that you create and assign to users are standalone. No inheritance occurs from one profile to another profile, including the Default profile.

When you associate a profile to a group, all users in the group have that profile added to their Allowed Profiles list. The profile is stored with the user, not the group. If a user is later added to the group, they will not be assigned the profile that was earlier assigned to the users of the group.

You can also designate any profile as the default profile or fallback profile. For more information, see ["Setting default and fallback profiles" on page 221](#).

Important:

- If you assign a user to a different profile, the change becomes effective immediately with no action required on the part of the user. While a user is logged in, you can assign different profiles to the user but you should not change their "Current Profile" or remove it from the list of "Allowed Profiles" because that may result in the user losing unsaved work.
- Users can change from one assigned profile to another themselves. For more information, see "Changing your profile" in the *IBM OpenPages with Watson User Guide*.

You can associate available objects with any profile and disassociate them later. However, each profile contains a group of required objects that you cannot disassociate from the profile. The following table lists these required object types:

Table 101. Required object types	
Object Type	Label
SOXBusEntity	Business Entity
SOXSignature	Signature
SOXExternalDocument	Link (this is an external URL link)

Guidelines for working with profiles

Following are some suggested guidelines for working with profiles.

- Create and enable a default profile and a fallback profile before you create any other profiles. For more information, see ["Setting default and fallback profiles" on page 221](#).
- Consider designating the most commonly used profile as the default profile.
- Do not disable, delete, or disassociate profiles that users are actively using because this might disrupt their work. In particular, do not do so unless you have created and enabled a fallback profile that users with no other active profile can use.

- Associate one or more new profiles to a user or group before disabling or deleting all of their existing ones.

Accessing profiles

From a profile, you can modify profile information, associate users and groups, and associate reports.

Before you begin

Log on to IBM OpenPages with Watson as a user with the Profiles application permission set. For more information, see [“Types of application permissions” on page 52](#).

Procedure

Click  > **Solution Configuration** > **Profiles**.

Creating a profile

You can create a new profile based on an existing profile, including the **Default** profile that is supplied with the product.

Procedure

- Click  > **Solution Configuration** > **Profiles**.
- Click **New Profile**.
- Enter a **Name** for the profile. The name should be easily recognizable by users and identify the purpose for which it is designed. Profile names cannot be translated or changed after they are created.
- Enter a **Description**.
- Click **Based on Profile** and select a profile to use as a template for the new profile.
- If you want the new profile to be the default profile, select **Default**. For more information, see [“Setting default and fallback profiles” on page 221](#).

Important: Creating a default profile might affect the way IBM OpenPages with Watson handles objects and profiles.

- If you want the new profile to be the fallback profile, select **Fallback**. For more information, see [“Setting default and fallback profiles” on page 221](#).
- Select **Enabled**.
- Optional: Enter or change the name and description of the profile for each locale.
- Click **Done**.

The profile is created and added to the list of profiles.

- Click the name of the profile and finish configuring the profile by completing following tasks:

Table 102. Profile configuration tasks

To ...	See this topic ...
Associate and disassociate users and groups	“Associating users to a profile” on page 224 and “Associating groups to a profile” on page 224 “Disassociating users from a profile” on page 225 and “Disassociating groups from a profile” on page 225

Table 102. Profile configuration tasks (continued)

To ...	See this topic ...
Include and exclude object types	“Including object types in a profile” on page 226 “Removing object types from a profile” on page 226
Associate reports	“Adding reports to a profile” on page 227

Setting default and fallback profiles

You can set a default profile and fallback profile.

About this task

This task is optional, but it's a good practice to set a default profile and a fallback profile.

Before you set a default or fallback profile, see [“Guidelines for working with profiles” on page 219](#).

Default profile

When you create a user, the user's **Current profile** is set to the default profile. You can then change the user's current profile, if needed.

You can use any profile as the default profile, and there can be only one default profile. Choose a profile that you'll use most often for new users.

If you don't designate a default profile, the **Default** profile is used. The **Default** profile is included with OpenPages. This profile does not give access to any object types, dashboards, or reports.

All profiles are standalone; there is no inheritance from the default profile to other profiles.

Fallback profile

The fallback profile is used when a user has no other enabled profiles available.

The fallback profile allows a user who is either not associated with any profile, or whose profile is disabled or deleted, to log in to OpenPages.

Only one profile can be set as the fallback profile. When you set a profile as the fallback profile, the existing fallback profile (if there is one) loses this designation.

The fallback profile is optional, however it's a good practice to set and enable one so users without any other enabled profiles can log in.

Procedure

1. Click  > **Solution Configuration > Profiles**.
2. Click the name of a profile.
3. Click **Edit**.
4. On the **Edit Profile** page, select one or both of the following options:
 - **Default** - to make this profile the default profile
 - **Fallback** - to make this profile the fallback profile
5. Select **Enabled**.
6. Optional: Enter or change the description of the profile.
7. Optional: Enter or change the name and description of the profile for each locale.
8. Click **Done**.

Editing a profile

You can modify the description of a profile or designate the profile as the default profile or fallback profile.

Procedure

1. Click  > **Solution Configuration > Profiles**.
2. Click the name of a profile.
3. Click **Edit**.
4. Make your edits.
Note that a profile name cannot be changed after the profile is created. But you can edit the names and descriptions for the locales.
5. Click **Done**.

Deleting a profile

You can delete a profile.

Important: If you delete a profile, it immediately disappears from the system and you cannot retrieve it. It is immediately unavailable to currently logged in users or to users who subsequently log in. If you are not sure if you might need the profile again, disable it instead.

Before deleting a profile, see “[Guidelines for working with profiles](#)” on page 219.

For users with multiple profiles, the current profile becomes the first profile in the alphabetical list of their allowed profiles. If you delete the only profile that is assigned to a user, the user can still log in using the fallback profile if one exists and is enabled. For more information, see “[Setting default and fallback profiles](#)” on page 221

Procedure

1. Click  > **Solution Configuration > Profiles**.
2. Select the box next to each profile you want to delete.
3. Click **Delete**.
4. Click **Delete** to confirm the deletion.

Enabling a profile

When you enable a profile the status of the profile changes from Inactive to Active, and the profile immediately becomes available to users who are assigned that profile (either currently logged on users or to users who subsequently log on).

Procedure

1. Click  > **Solution Configuration > Profiles**.
2. Click the name of a profile.
3. Click **Edit**.
4. Click **Enable**.

The status changes to **Active**.

Alternatively, from the list of profiles, you can select the box next to one or more profiles and click **Enable**.

Disabling a profile

You can disable a profile.

Important: When you disable a profile, it is not deleted. It remains in the system, and the status of the profile changes from Active to Inactive. A disabled profile is immediately unavailable to users to currently logged in users or to users who subsequently log in.

Before disabling a profile, see “[Guidelines for working with profiles](#)” on page 219.

For users with multiple profiles, the current profile becomes the first profile in the alphabetical list of their allowed profiles. If you disable the only profile that is assigned to a user, the user can still log in using the fallback profile if one exists and is enabled. For more information, see “[Setting default and fallback profiles](#)” on page 221.

Procedure

1. Click  > **Solution Configuration** > **Profiles**.
2. Click a profile name.
3. Click **Edit**.
4. Click **Disable**.

The status changes to **Inactive**.

Alternatively, from the list of profiles, you can select the box next to one or more profiles and click **Disable**.

Associating profiles to a user

You can associate one or more profiles to a user or group. Having multiple profiles is beneficial for users that have more than one function and require a different profile for each one. It is also beneficial for administrators because it can reduce the number of profiles that they need to create and maintain.

Tip: It is more efficient to associate profiles to groups rather than individual users. Note that if a user is later added to the group, they will not be assigned the profile that was earlier assigned to the users of the group.

This video demonstrates how to associate profiles with a user:

<https://youtu.be/59SRFnLdrj4>

About this task

The following steps explain how to associate profiles from a user account. You can also associate profiles to users and groups from the profile page. For more information, see “[Associating users to a profile](#)” on page 224 and “[Associating groups to a profile](#)” on page 224.

Note that from a group, it is not possible to assign a group to a profile. You must go to the profile page and assign a group to the profile.

Procedure

1. Click  > **Users and Security** > **Users**.
2. Select the user that you want to assign a profile to.
3. In **Allowed Profiles**, select all the profiles that you want to assign to the user.
4. Optionally, you can change the user's current profile by selecting a different profile from the **Current Profile** list.

Warning: If you change a user's profile while they are logged on you might disrupt their work.

- If you remove the user's current profile from **Allowed Profiles**, the user's current profile is set to the first allowed profile in the alphabetical list.
 - For existing users, the **Current Profile** is set to the user's current profile.
 - For new users, the current profile is set to the default profile, if one exists and is enabled. If an enabled default does not exist, the current profile is set to the fallback profile, if one exists and is enabled. For more information, see “[Setting default and fallback profiles](#)” on page 221.
5. Click **Save**. The changes take effect immediately.

Associating users to a profile

You can associate users to one or more profiles. Users that have no associated profiles use the fallback profile, if one exists.

For more information, see “[Setting default and fallback profiles](#)” on page 221.

When you associate a profile with a user, the object types in that profile are available to that user. Additionally, you can select the fields within each object type that users of this profile can view.

The profile that you associate with a user is not the current profile unless no current profile is selected.

<i>Table 103. Associating users to a profile</i>	
If you select a...	Then this occurs...
user who has no profile	the currently selected profile is assigned to that user.
user who already has a profile assigned	the current profile stays the same, and the new profile is added to their list of allowed profiles.

About this task

The following steps explain how to associate users to a profile on a profile page. You can also associate profiles from the user account. For more information, see “[Modifying user accounts](#)” on page 49 and “[Associating profiles to a user](#)” on page 223.

Procedure

1. Click  > **Solution Configuration** > **Profiles**.
2. Click the name of a profile.
3. Go to the **Users** section.
4. Click **Add**.
5. Search for the user or group that you want to add.

If you specify a group, all users in the group have that profile added to their **Allowed Profiles** list. The profile is stored with the user, not the group. If a user is disassociated from a group, the profile is not disassociated from the user. If a user is later added to the group, they are not assigned the profile that was earlier assigned to the users of the group.

To associate a group to a profile directly, see “[Associating groups to a profile](#)” on page 224.

6. Select it.
7. Click **Done**.
8. Repeat the steps for the next user.

Associating groups to a profile

You can associate groups to one or more profiles.

When you associate a profile to a group, all users in the group have that profile added to their **Allowed Profiles** list. If you add a user to a group on the group's administration panel, the user gets the object

profile on the Allowed group profiles list automatically. If the user is removed from a group, the indirect association to the profile is removed automatically.

About this task

The following steps explain how to associate groups to a profile on a profile page.

Procedure

1. Click  > **Solution Configuration > Profiles**.
2. Click the name of a profile.
3. Go to the **Groups** section.
4. Click **Add**.
5. Search for the group that you want to add.
6. Select it.
7. Click **Done**.
8. Repeat the steps for the next group.

Disassociating users from a profile

When you disassociate a user from a profile, that profile becomes immediately unavailable to that user unless they belong to another group that is associated with the profile.

If the user has only one allowed profile after the disassociation, that profile becomes their current profile. If the user has multiple profiles after the disassociation, a profile selection panel is displayed to the user at the next login to OpenPages. The profile that the user selects becomes the user's current profile. If the user has no other available profiles, the fallback profile is used. If no fallback profile is assigned, the user is unable to log on to the application. For more information, see [“Setting default and fallback profiles” on page 221](#).

Before disassociating a user from a profile, see [“Guidelines for working with profiles” on page 219](#).

About this task

You can disassociate users from a profile. Alternatively, you can disassociate users from profiles from the user account. For more information, see [“Modifying user accounts” on page 49](#).

Procedure

1. Click  > **Solution Configuration > Profiles**.
2. Click the name of a profile.
3. Go to the **Users** section.
4. Select the user with a checkmark.
5. Click **Remove**.
6. Click **Remove** again to confirm.

Disassociating groups from a profile

When you disassociate a group from a profile, that profile becomes immediately unavailable to all users in that group except under the following conditions.

- The profile remains available to users who belong to another group that is associated with the profile.
- The profile remains available to users who are individually associated with the profile.

Before disassociating a group from a profile, see [“Guidelines for working with profiles” on page 219](#).

About this task

You can disassociate a group from a profile.

Procedure

1. Click  > **Solution Configuration > Profiles**.
2. Click the name of a profile.
3. Go to the **Groups** section.
4. Select the group with a checkmark.
5. Click **Remove**.
6. Click **Remove** again to confirm.

Including object types in a profile

When you include an object type in a profile, that object type is immediately visible to users who are assigned the selected profile. The object types that you select determine which menus appear and the contents of each menu.

Procedure

1. Click  > **Solution Configuration > Profiles**.
2. Click the name of a profile.
3. Go to the **Object Types** section.
4. Click **Add**.
5. Select the box next to each object type to add to the profile.
6. Click **Done**.

Removing object types from a profile

When you remove (exclude) an object type from a profile, that object type is removed from the views in which it is used. It is no longer available to users who are assigned that profile.

Note: Certain object types are required. You get an error message if you try to remove them.

Procedure

1. Click  > **Solution Configuration > Profiles**.
2. Click the name of a profile.
3. Go to the **Object Types** section.
4. Select the box next to each object type that you want to remove from the profile.
5. Click **Remove**.
6. Click **Remove** again to confirm.

Results

The selected object type is removed from the list of object types for this profile. IBM OpenPages with Watson stores an excluded object, along with any associated data, in the repository. You can view it through reports.

Adding reports to a profile

When you add reports to a profile, users can add those reports to their Dashboard.

Procedure

1. Click  > **Solution Configuration > Profiles**.
2. Click the name of a profile.
3. Go to the **Reports** section.
4. Click **Add**.
5. Select each report to add to the profile.
6. Click **Done**.

Results

The reports are added to the profile and enabled.

You can hide reports from dashboards by disabling the reports in the profile. Or, you can remove the report from the profile. Select the report and then click **Disable** or **Remove**.

Including fields in an object type

Including object fields for an object type in a profile makes those object fields available for selection within the various views.

The availability of a field for configuration within any view depends on whether that field is included or excluded in the object type for that profile. Including or excluding fields for object types in one profile does not affect object-type fields in other profiles.

Procedure

1. Click  > **Solution Configuration > Profiles**.
2. Click the name of a profile.
3. Go to the **Object Types** section.
4. Click the name of the object type whose fields you want to modify (for example, SOXIssue).
5. Expand the **Fields** section.
6. Click **Add**.
7. Select the fields to add to the profile and click **Done**.
8. After it is added to the list of fields, click the field name.

The **Profile Field Configuration** panel opens. On this panel, **Display Type** is set and cannot be changed. Depending on the field type, additional fields might be available. For example, for user fields, the following fields can be set:

- **Include Disabled**
- **Starting Group**
- **Minimum Access** (Read, Write, Delete, Associate).

9. Click **Done**.

Excluding fields from an object type

Excluding an object field from an object type in a profile immediately removes that object field from the views in which it is used, and that field is no longer available for configuration in a view or to users who are assigned that profile.

The availability of a field for configuration within any view depends on whether that field is included or excluded in the object type for that profile. Including or excluding fields for object types in one profile does not affect object-type fields in other profiles.

Procedure

1. Click  > **Solution Configuration** > **Profiles**.
2. Click the name of a profile.
3. Go to the **Object Types** section.
4. Click the name of the object type whose fields you want to modify (for example, SOXIssue).
5. Expand the **Fields** section.
6. Select the check box next to the field to exclude and click **Remove**.
7. Click **Remove** again to confirm.

Results

The excluded object fields are now absent from the list of available fields for this object type in this profile.

Setting a field in a profile to required or optional

You can set a specific field to required or optional for a profile and object type.

Setting a field to required in a profile affects only the users who are assigned that profile.

Note: If a field is not listed in the **Object Fields** pane, you must include it before you can modify it (see “[Including fields in an object type](#)” on page 227).

Procedure

1. Click  > **Solution Configuration** > **Profiles**.
2. Click the name of a profile.
3. Go to **Object Types**.
4. Click the name of the object type that has the field to modify.
5. Go to the **Fields** section.
6. Click the name of the field to modify.
The **Profile Field Configuration** panel opens.
7. Set **Required** to True or False.
8. Click **Done**.

Chapter 13. Configuring the UI

The OpenPages user interface is used by users and risk managers who need find information and complete tasks that are assigned to them.

Setting up the UI

Before users can access the user interface, you must configure who can access it and define the views that are available.

Before you begin

Complete the following prerequisites:

- Learn about how users can interact with the user interface. For more information, see *Getting started with the UI* in the *IBM OpenPages with Watson User Guide*.
- Learn about views and how they are defined in the View Designer. For information, see [Chapter 14, “Views,” on page 247](#) and [“Using the View Designer” on page 272](#).
- Learn about the GRC Workflow feature and plan how you will use it. Configure it after you configure the UI with the exception of Task Views and Admin Views, which can be designed concurrently. For information, see [“Setting up GRC Workflow” on page 369](#).

About this task

During the configuration process, plan and design what you want users to accomplish in the UI. After configuring the UI, you can define views that allow users to interact with OpenPages in a way that is tailored to your requirements.

Procedure

1. Update the permissions for role templates for administrators who are configuring the UI.

a) Click  > **Users and Security** > **Role Templates**.

b) Click a role template, and go to the **Role Permissions** section.

c) Click **Edit**.

d) Select the **SOX > Administration > Task Focused UI** permission.

Administrators with this permission can define views with the  > **Solution Configuration** > **Views** task in the UI.

In addition to **Views**, this permission also controls whether the  > **Other** > **Display Debug Info** task is displayed.

e) Select the **SOX > Administration > Dashboards** permission.

Administrators with this permission can define dashboards with the  > **Solution Configuration** > **Dashboards** task in the UI.

2. No changes are required to the permissions for role templates for users who access the UI. All users have access to the UI.
3. Review profiles for users who will use the UI.
4. Define default dashboards for profiles. For more information, see [“Home page, dashboard, and tabs” on page 230](#) and [“Defining a dashboard for a profile” on page 231](#).
5. Create the views that are used in the UI. For information, see [Chapter 14, “Views,” on page 247](#).
6. Optional: Customize the Primary menu.

For more information, see “Customizing the Primary menu” on page 233.

7. Optional: Configure IBM Watson components that are used with OpenPages. For more information, see Chapter 33, “Configuring IBM Watson Integrations,” on page 843.
8. Optional: Configure a Net Promoter Score survey. For more information, see “Configuring a Net Promoter Score survey” on page 239.

Home page, dashboard, and tabs

The Home page is the initial page that is displayed to users see when they log in to OpenPages.

The Home page organizes information and tasks. It contains three parts:

- A dashboard
- Task tabs
- Tabs for reports

Dashboard on the Home page

The dashboard displays panels with content that is personalized for each user.

Dashboard panels in the UI can come from the following sources:

- Users can define their own dashboard panels in the UI. On the Home page, a user clicks  to open the Dashboard configuration menu.

For more information about how users add panels to the dashboard in the UI, see the *IBM OpenPages with Watson User Guide*.

- Administrators can define dashboards in the UI that apply to specific profiles. In this way, users have a default dashboard based on the profile that they belong to. The dashboards are consistent and standardized across a group of users. Users can still customize their dashboard by adding their own dashboard panels or hiding dashboard panels that are defined on the default dashboard.

For more information, see “Defining a dashboard for a profile” on page 231.

Task tabs on the Home page

The following task tabs display on the Home page:

- My Tasks tab

The My Tasks tab summarizes the tasks that belong to a user.

- Subscription Tasks tab

The Subscription Tasks tab summarizes the tasks that a user is subscribed to.

- Oversight Tasks tab

The Oversight Tasks tab summarizes the tasks for which a user has oversight responsibility.

The content and layout of each tab is fixed and cannot be changed. For more information about the task tabs, see the *IBM OpenPages with Watson User Guide*.

Tabs on the Home page for reports

A dashboard can contain up to three tabs for Cognos and OpenPages reports.

The reports must already exist and must be added to the profile. Two methods can be used to create tabs for reports: users can define report tabs on their dashboard and administrators can use the **Manage Dashboards** task.

For more information, see the *IBM OpenPages with Watson User Guide* and “Defining a dashboard for a profile” on page 231.

Improve performance

Each panel that you add to the Home page increases the work that is required to display that panel. A large number of panels can negatively impact performance.

To improve performance, limit the number of panels and use filters to restrict the data that is displayed on each panel.

The exact cost to fetch and display the data for each panel depends on a number of factors, for example, the data size, filter criteria, security rules, browser, and available system resources.

Defining a dashboard for a profile

A dashboard can contain multiple panels and up to three tabs for Cognos and OpenPages reports. A dashboard that is defined for a profile provides a default dashboard for all users that belong to that profile.

Before you begin

See the *IBM OpenPages with Watson User Guide* for information about configuring dashboard panels, including charts, filter counts, and other widgets in the UI.

Review the filters for object types that are used in dashboard panels. For a filter to be available in a dashboard panel, it must be associated to the object type. For more information, see “[Configuring filters for an object type](#)” on page 204.

Tip: Keep the number of panels on the dashboard reasonable. A dashboard with many panels can potentially take longer to load.

To add tabs for reports, the following conditions must be met:

- The reports must already exist in OpenPages. For more information about creating reports, see “[OpenPages platform reports](#)” on page 125.
- The reports must be added to the profile. For more information, see “[Adding reports to a profile](#)” on page 227.

About this task

A dashboard must be marked as active for the panels to appear on users' dashboards.

Multiple dashboards can exist for that same profile. If more than one dashboard is marked as active, the last published dashboard is the one that is displayed on users' dashboards.

Click  to access a search filter. You can search by the active setting and profile. You can also click in the search box and enter free text. The search box is based on dashboard name, profile, and description.

Dashboards can be migrated from one environment to another environment using Export Configuration and Import Configuration or the ObjectManager tool. For more information, see “[Exporting and importing dashboards](#)” on page 241.

Procedure

1. Click  > **Solution Configuration** > **Dashboards**.
2. Click **New Dashboard**.
3. Enter a **Name**. Allowed characters are A-Z, a-z, 0-9, underscore, hyphen, and spaces. Special characters are not allowed.
4. Set **Active** to **True** or **False**.
5. Select a **Profile** that the dashboard applies to.
6. Optional: Enter a **Description**.
7. Click **Create**.

The dashboard is added to the list of dashboards.

8. Click the dashboard name.

9. Click  to open the Dashboard configuration menu.

10. Click **New Panel** and begin defining the panels for the dashboard. See the *IBM OpenPages with Watson User Guide* for more information.

For some panel types, you can use filters. The filters list displays the public filters that are defined for the object type.

11. Click **Add Report Tab** to add tabs for reports.

a) Enter a **Name**.

b) Enter a **Label**. Keep it short. Click **Edit** to enter localized values.

If it is displayed, click  to populate translated values to languages. For more information, see “[IBM Watson Language Translator](#)” on page 847.

c) Select a **Report**.

d) Click **Done**.

The report tab is added. A dashboard can have up to three report tabs. Click a tab and move it to where you want it to display. Tabs can be removed, if needed.

12. Click **Done**.

13. Click **Publish**.

14. Test the dashboard. Each time you change the dashboard, you need to publish it and retest it.

Changes to profiles can affect dashboards. If an object type, filter, or chart field is removed from a profile, the dashboard panels and content will change. If the profile change affects a panel as a whole, for example, an object type is removed from a profile, then the panel is removed. If the profile change affects only a single widget in a custom panel, then the widget is removed. This can cause an empty panel to display on a dashboard. You can either repopulate the custom panel with other widgets or delete it.

If the Dashboard encounters a problem and cannot render, you can apply safe mode by adding ?safeMode=1 to the end of the URL. The rendering process stops and you can access the dashboard configuration to debug the problem. Remove ?safeMode=1 from the URL to exit safe mode.

Adding a Search panel

A Search panel on a dashboard provides a means to use global search in the UI.

Before you begin

Global search is a powerful feature for finding information. To learn more about it, see the *IBM OpenPages with Watson User Guide*.

Global search must already be configured. For more information, see [Chapter 21, “Configuring the global search feature,” on page 517](#).

About this task

When a user enters text in a Search panel, global search analyzes the input and displays matching results, including the item title, description, and the item type. Up to 25 objects can be returned in a Search panel. If a user clicks an object in the Search panel result list, the object opens in a new tab. The user can also mark an object as a favorite.

Consider your usability and performance when you design the Search panels. A Dashboard may need to contain one Search panel that can search across all objects. It may also need one or more Search panels that are targeted to specific objects types that users access most frequently. For these Search panels, set values in **Object Type** and **Folder Picker** so that the search is restricted to a smaller set of objects.

Procedure

1. Create a dashboard panel and complete the steps up to adding a panel. For more information, see ["Defining a dashboard for a profile" on page 231](#).
2. Click **New Panel**.
3. Select **Search in Panel Type**.
4. Enter a **Name**. Allowed characters are A-Z, a-z, 0-9, underscore, hyphen, and spaces. Special characters are not allowed.
5. Enter a **Label**. The label displays as a title for the panel.
6. Set **Object Type** to *All object types* or select one or more object types to restrict the search to specific object types. Be sure to select **File** in **Object Type** if you want to include file attachments descriptions and content in the search.
7. Optional: Click **Choose** and select one or more folders in **Folder Picker**.
8. Click **Done**.
9. Click **Done**.
10. Click **Publish**.
11. Test the search panel. Each time you change the dashboard, you need to publish it and retest it.

What to do next

If it does not already exist, add a favorite objects panel to the dashboard so that users can access the objects they mark as favorites.

Customizing the Primary menu

You can customize the Primary menu so that you can quickly access the object types you work on most frequently.

- You can change the order of object types in the Primary menu and its submenus.
- You can add object types to a submenu.
- You can add a submenu that contains object types.

The menu items that are displayed depend on the user's profile and role template, and the configuration of the menu in Settings.

You cannot add system items, such as **Background Processes**, to the Primary menu.

If you use IBM Cognos Analytics, the **Analytics** menu item displays as the first item in the list. This placement cannot be changed.

If OpenPages is used with IBM OpenPages for IBM Cloud Pak for Data, the **Analytics** menu item does not display on the Primary menu.



Warning: The changes that you make might be lost when you upgrade IBM OpenPages with Watson. Like all customizations, include these changes when you back up your environment before an upgrade.

Changing the order of menu items

You can change the order of object types in the Primary menu and its submenus.

Procedure

1. Click > **System Configuration** > **Settings**.
2. Click **Applications** > **Common** > **Configuration** > **Show Hidden Settings** and set the value to **true**.
3. Click **Applications** > **GRCM** > **NavigationMenu**.

4. To change the order of top-level items, edit the **Items** setting under **NavigationMenu**. Change the order of items in the comma-separated list.

Note: The following items are not displayed in the UI:
MyOpenPages, Reports, IncidentManagement, Administration

For example, if you move Vendors after Organization, the Primary menu looks like this:

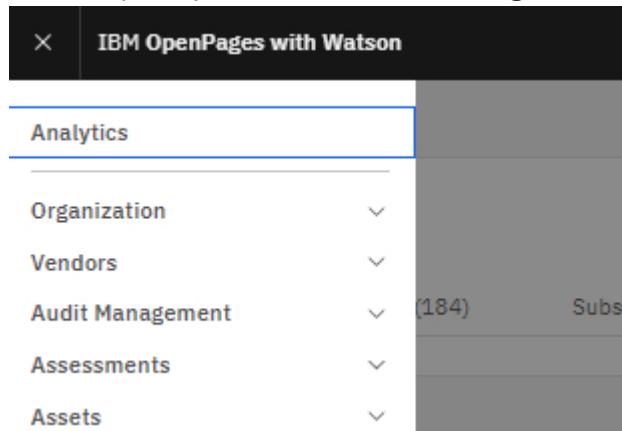


Figure 14. Reordering menu items

You might need to refresh the page or log out and log in to see your changes.

5. To change the order of items in a submenu, expand the folder for the submenu, and then edit the **ObjectTypes** setting.

For example, suppose that you want **Contracts** to be the first item in the **Vendors** submenu. To do this, expand the **Vendors** folder, click the **ObjectTypes** setting, and put Contract first in the list of object types. The Primary menu looks like this:

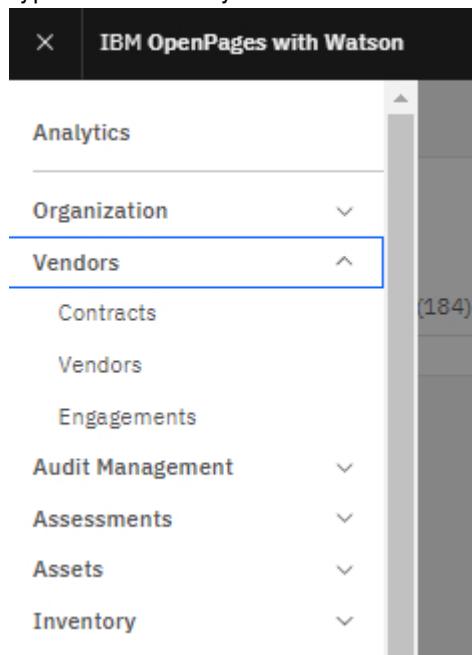


Figure 15. Reordering menu items

You might need to refresh the page or log out and log in to see your changes.

Results

The Primary menu is updated.

Adding object types to a submenu

You can add object types to a submenu in the Primary menu.

Procedure

1. Click  > **System Configuration** > **Settings**.
2. Click **Applications** > **Common** > **Configuration** > **Show Hidden Settings** and set the value to true.
3. Click **Applications** > **GRCM** > **NavigationMenu**.
4. Expand the folder where you want to add the object types.

For example, if you want to add an object type to the **Vendors** submenu, expand the **Vendors** folder.

5. Edit the **ObjectTypes** setting. Add the object types to the comma-separated list, in the order in which you want them to appear.

For example, to add **Files** to the **Vendors** submenu, add SOXDocument to the list.

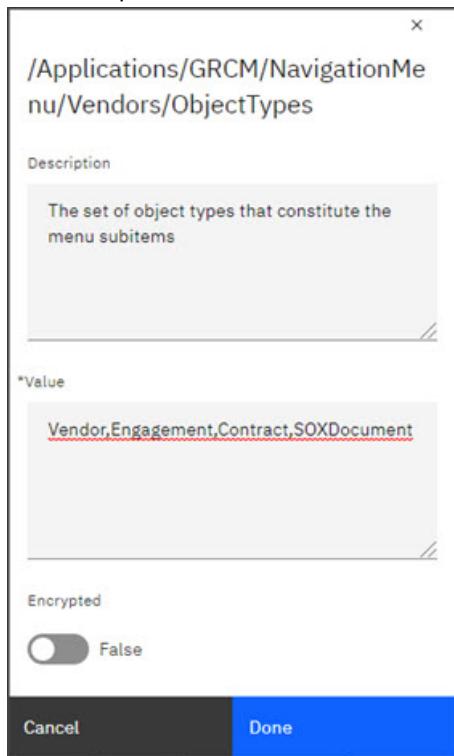


Figure 16. Adding SOXDocument to the ObjectTypes setting

The Primary menu looks like this:

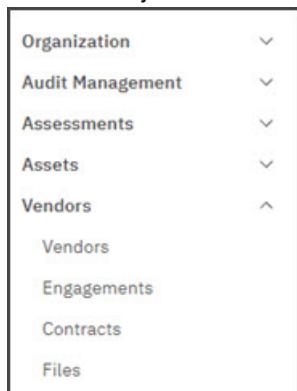


Figure 17. Adding Files to the Vendors menu

You might need to refresh the page or log out and log in to see your changes.

Note: If you don't see the object, check the **Applications > GRCM > NavigationMenu > Administration > Schema > SpecialObjectTypes > ObjectTypes** setting. If the object is listed, remove it.

Results

The Primary menu is updated.

Creating a new top-level menu item

You can add a top-level menu item that contains object types.

Procedure

1. Click  **System Configuration > Settings**.
2. Create an application text string for your new top-level menu.
See [“Adding new keys” on page 455](#).
For example, create an application text string called Test and set its default value to **Files & Links**.
3. Click **Applications > Common > Configuration > Show Hidden Settings** and set the value to **true**.
4. Click **Applications > Common > Configuration > Allow Create and Delete Settings** and set the value to **true**.
5. Click **Applications > GRCM**.
6. Click the check box next to the **NavigationMenu** folder, and then click **New Folder**. Type a folder name.
Users do not see the folder name in the user interface.
For example, create a folder called **TestFolder**.
7. Refresh the page.
The folder that you created is now visible.
8. Click the check box next to the new folder that you created in step 6. Click **New Setting**.
9. Add a setting called **ObjectTypes** and set the value to a comma-separated list of object type names
For example: **SOXDocument, SOXExternalDocument**
10. Add another setting. Name it **TextKey** and set its value to the application text string that you created in step 2.

<input type="checkbox"/>	 TestFolder
<input type="checkbox"/>	ObjectTypes
<input type="checkbox"/>	TestKey

Figure 18. Adding the application text string for the new submenu

11. In the **Items** setting under **NavigationMenu**, add the name of the folder that you created. Put the folder name in the order where you want it to display in the Primary menu.

For example, add **TestFolder** after **Organization**.

The Primary menu looks like this:

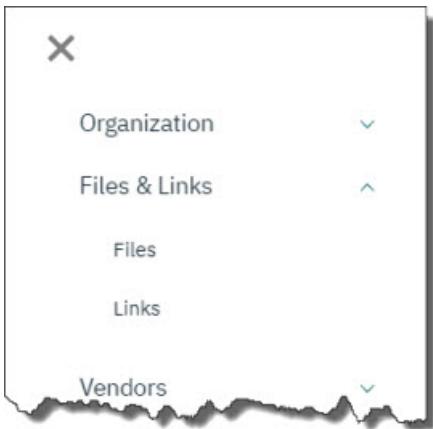


Figure 19. Adding the submenu

Remember: The submenu name is defined by the application text string that you created in step 2. If you're following the examples, you see **Files & Links**, the value of the Test application text string.

You might need to refresh the page or log out and log in to see your changes.

Results

The Primary menu is updated.

Creating tags

In OpenPages, users can use tags to categorize objects and perform searches based on those categories.

Before you begin

You must have the All Permissions/SOX/Administration/Tagging permission to enable and disable the Tagging feature, and create, edit, and disable tags.

Tag names cannot contain the following characters:

```
* (asterisk)
! (exclamation mark)
# (number sign)
< (less-than)
> (greater-than)
; (semicolon)
' (single quote)
" (double quotes)
` (back quote)
@ (at)
$ (dollar)
% (percentage)
^ (caret)
~ (tilde)
+ (plus)
= (equals)
| (pipe)
? (question mark)
, (comma)
. (period)
```

The number of tags in the system is limited to 500.

Procedure

1. Click > **Solution Configuration** > **Tags**.
2. Click **New tag**.

3. Enter a **Name** for the tag.
Tag names are limited to 30 characters.
4. Optional: Enter a **Description** for the tag.
Tag descriptions are limited to 100 characters.
5. Click **Create**.
6. Optional: If you want to enable tagging so that users can view and add tags, select **Tagging is enabled** in the **System settings** panel, and click **Enable**.
7. Optional: By default, users can apply tags to all object types. If you want to prevent the application of tags to specific object types, click the **Enable tagging for these object types** box and ensure that the object types selected are the object types that you want to have tags. If you want to disable tagging for an object type, deselect it.

Integrating WalkMe

WalkMe is a third-party tool that integrates with OpenPages to deploy custom content and provide guidance to new users. Through guided tours, feature overviews, and embedded resources, WalkMe helps users make the most out of their OpenPages implementation.

About this task

Registry settings are embedded so that you can enable WalkMe and connect to your own WalkMe JavaScript snippets.

An implementation of WalkMe is integrated with OpenPages and enabled by default. If you want to disable WalkMe, follow step 1 of this task and set **Walkme Enabled** to **false**.

For custom implementations, you must have a separate license for WalkMe. For more information about WalkMe, see the [WalkMe web site](#).

WalkMe is available only for on-premises and SaaS deployments. WalkMe is not available on Cloud Pak for Data deployments.

Procedure

1. To see the registry settings for Walkme, perform the following steps:
 - a) Click  > **System Configuration** > **Settings** and set **Applications** > **Common** > **Configuration** > **Show Hidden Settings** to **true** to show hidden settings.
 - b) Go to **Applications** > **Walkme**.
- The following settings are displayed:

Settings (3)	
Name	Description
<input type="checkbox"/> WalkMe Enabled /Applications/WalkMe/WalkMe Enabled	Walkme onboarding/walk-thrus enabled (true/false)
<input type="checkbox"/> WalkMe URLs /Applications/WalkMe/WalkMe URLs	URLs of the embedded WalkMe script, space-separated and formatted for use in Content-Security-Policy less
<input type="checkbox"/> WalkMe Source /Applications/WalkMe/WalkMe Source	URL of WalkMe content

Figure 20. Configuring the Walkme application settings

2. To enable Walkme, set **Walkme Enabled** to true.
3. Configure firewalls to allow the domain names listed in **Walkme URLs**.
 The value of the **Walkme URLs** setting lists domains to allow for content security. For example, WalkMe flows can contain YouTube video contents that might be blocked by default due to content security. To allow YouTube contents, an administrator can enter a specific YouTube URL in the **Walkme URLs** setting. It is not recommended to enter the URL for the YouTube home page (<https://www.youtube.com/>) because it is less secure. If a YouTube URL is not specified, videos might not load and you might see a console error referring to CSP.
4. If you want to use your own WalkMe implementation, update **Walkme Source** to the URL for your JS snippet.
 By default, **Walkme Source** is set to the URL of IBM's cloud storage.

Configuring a Net Promoter Score survey

A Net Promoter Score (NPS) survey enables users to send feedback about OpenPages to IBM.

Before you begin

Ensure that your firewall allows users access to the survey. Review the URL to Medallia, the Net Promoter Score survey provider. For more information, see [“Reviewing the Net Promoter Score \(NPS\) survey settings” on page 490](#).

About this task

In fresh installations, NPS is enabled by default. Also, if you upgrade from a version prior to NPS being available, NPS is enabled by default.

When a Net Promoter Score survey is enabled, users are presented with two possibilities to complete a survey:

- An NPS **Feedback** button
- An NPS survey form on log in

An NPS Feedback button is always displayed on the Home page for users who are eligible to receive a survey. Users can provide feedback at any time and as often as they want.

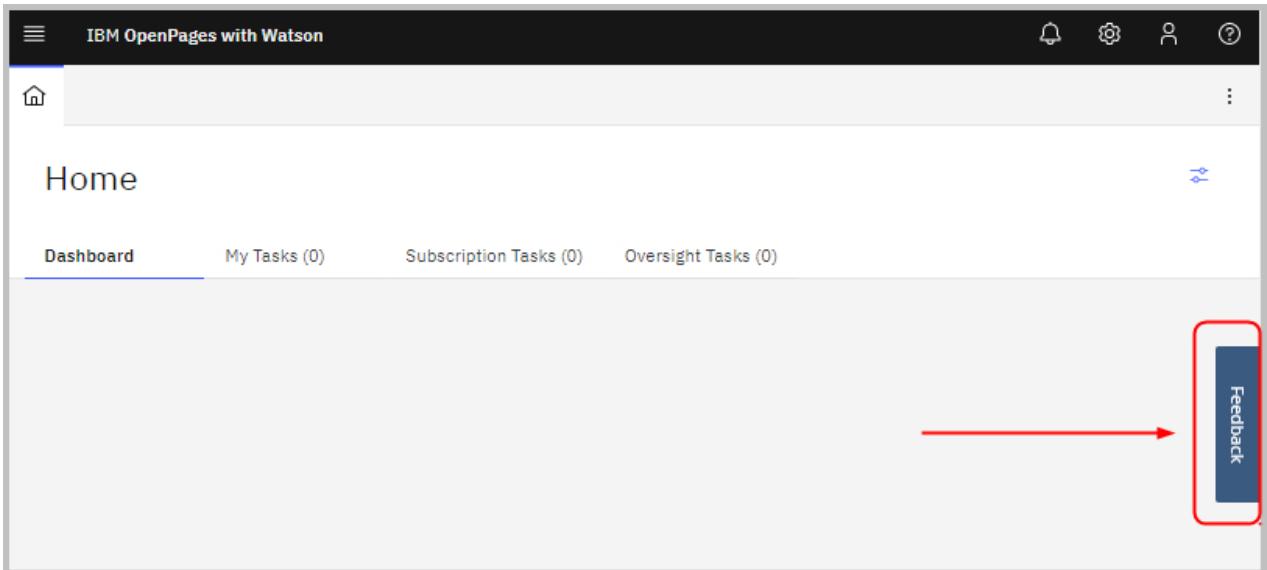


Figure 21. NPS Feedback button on the Home page

An NPS survey form is displayed on log in to users who meet the following conditions:

- The user must be eligible to receive the survey, as defined in **Included Users or Groups** and **Excluded Users or Groups**.
- The user must meet the Medallia frequency requirements:
 - The user was last presented with a survey at least 90 days ago. This prevents the survey from being presented too frequently. It is presented regardless of whether the user provided feedback or declined to provide feedback on the last survey.
 - The user must have logged in at least 30 days ago. This prevents the survey from being presented to brand new users.

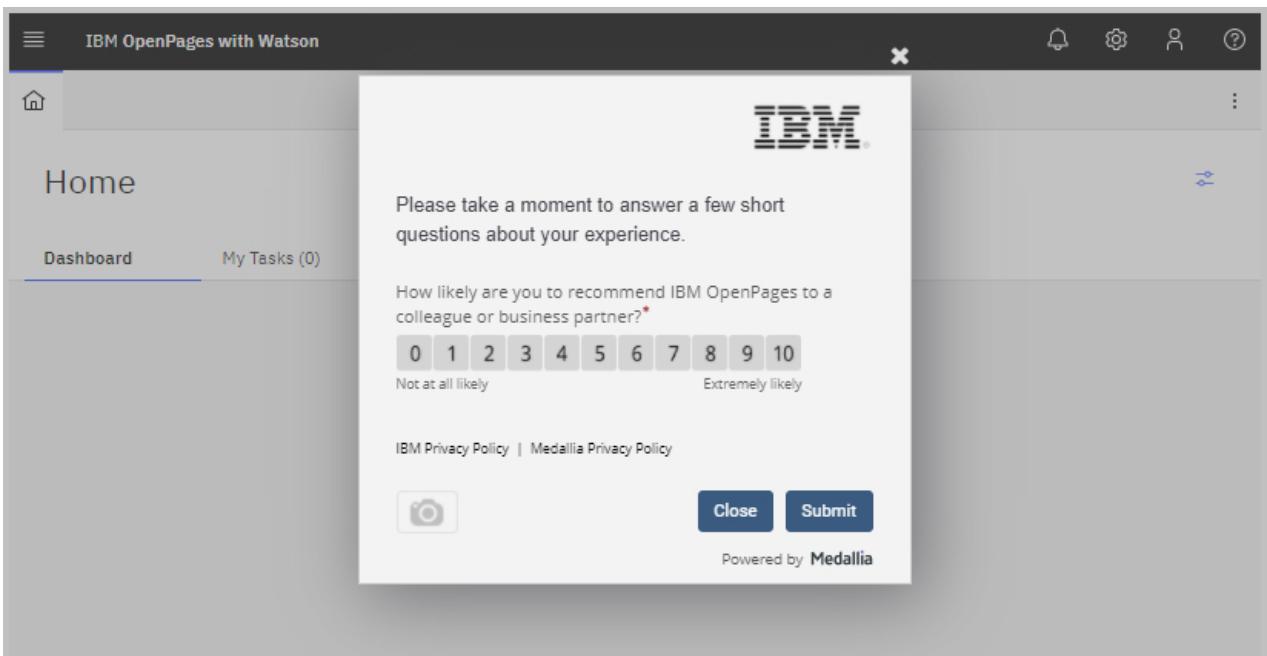


Figure 22. NPS survey form displayed after logging in

Procedure

1. Click  > **Integrations** > **NPS Settings**.
2. Set **Enable User Feedback Survey** to true. The default is false.
3. Enter your **IBM Customer Number (ICN)**.
4. Set **Percentage of Users to Target** to light (15%), medium (50%), or heavy (100%).
5. In **Included Users or Groups**, build the group of users who are eligible to receive a survey. If empty, all users are eligible to receive a survey.
6. In **Excluded Users or Groups**, add the users or groups who explicitly never receive a survey.
7. Click **Submit**.

Exporting and importing dashboards

You can migrate dashboards from one environment to another environment using Export Configuration and Import Configuration.

Before you begin

Read [Chapter 26, “Migrating OpenPages environments,” on page 719](#) to ensure that you are familiar with how to use Export Configuration and Import Configuration.

About this task

Dashboards are exported or imported as part of the profile that they belong to.

You can migrate dashboards that have been defined per profile by an administrator with the  > **Solution Configuration** > **Dashboards** task.

When you export dashboards using Export Configuration, the dashboards for the profiles you select are exported to a migration file.

Panels that users have manually added to their dashboard are excluded.

An alternative to using Export Configuration and Import Configuration is to use the ObjectManager tool. For more information, see [“Migrating configuration changes” on page 763](#).

Procedure

1. Follow the instructions described in [“Exporting and importing dashboards ” on page 241](#) and choose the profiles to export.
2. Follow the instructions described in [“Importing a migration file ” on page 729](#) to import the migration file into a target environment.
3. Access and test the dashboards in the target environment. Verify that the content of the dashboards is correct.

Themes

Themes are used to customize the colors that are displayed in OpenPages. Users can apply a theme by using the  > **Change Theme** task.

There are two types of themes:

- System themes
- Custom themes

System themes

There are four system themes, listed from lightest to darkest:

- Carbon White
- Carbon Gray 10 (default)
- Carbon Gray 90
- Carbon Gray 100

The system themes have defined colors. Carbon White and Carbon Gray 10 are light themes, while Carbon Gray 90 and 100 are dark themes.

The system themes are associated with two palettes:

- Categorical Palette
- Monochromatic Palette

Palettes contain colors that you can apply to enumerated string fields and numeric field ranges in charts and in views in the View Designer.

The colors in the system themes and the palettes cannot be changed.

Custom themes

Administrators can create their own themes, called custom themes. Initially, a custom theme must be based on an existing theme. Then you can design the theme and apply colors that meet your needs. You can, for example, apply colors that identify your company's color palette. Custom themes can be the default, enabled, disabled, and deleted.

Custom themes do not include their own palettes. Custom themes that are based on a light theme are combined with colors from the light set of colors in the Categorical Palette. Custom themes that are based on a dark theme are combined with colors from the dark set of colors in the Categorical Palette. For more information about applying colors to fields, see [“Supported color palettes for field values” on page 159](#).

Carbon

Colors in the system themes and the palettes used in OpenPages are based on Carbon. For more information, see <https://www.carbondesignsystem.com/guidelines/color/overview>.

IBM Watson Assistant

If IBM Watson Assistant is used, a selected theme is automatically applied to the chat bot.

Theme list

Use the  > **Solution Configuration** > **Themes** task to work with themes.

The Theme List shows themes that are defined. From the Theme List, you can:

- Click a theme. The theme opens and you can view it or make changes.
 - A system theme can be enabled, disabled, or designated as the default. Otherwise, no changes are allowed. They cannot be deleted.
 - A custom theme can be enabled, disabled, deleted, designated as the default, and colors can be changed.
- To change the default theme, select **Default**. It is not possible to clear the **Default** check box on a theme, instead, mark another theme as the default. Only one theme can be the default.
- To enable a theme, select **Enabled**. All enabled themes are displayed to users for selection on the  > **Change Theme** task. Enable only one theme to not allow users to change the theme. There is no application permission for the  > **Change Theme** task.
- Select the check box next to a single theme or multiple themes to update numerous themes. The bulk update options are:

- Delete
- Enable
- Disable

System themes cannot be deleted.

Clear the check boxes to hide the bulk update options.

- Click **Add Theme** to create a new theme. For more information, see “[Defining custom themes](#)” on page 243.
- Click the **Name** column header to change the sort order of the list.

Users apply themes

After themes have been configured, users can click  > **Themes** and apply a theme. Any system or custom theme that is enabled is available for selection. The default theme is applied if they do not apply a theme.

Restrictions

The following restrictions exist for themes:

- Theme selection is retained the next time a user signs in, regardless of browser.
- Themes are not applied to:
 - The login page. The login page always uses the Carbon Gray 10 theme.
 - The page header and menus. They are always black/white.
 - Questionnaires.
 - Helpers.

Defining custom themes

Custom themes contain a color scheme that is designed for your organization.

Before you begin

Review the existing themes and decide which one is the best base for the new custom theme.

To do this task, you need the **SOX > Administration > Solutions** application permission.

About this task

Design the theme and apply colors that meet your needs. The following table lists the settings you can use.

<i>Table 104. Color settings</i>	
Color setting	UI elements the setting applies to
background-brand	<ul style="list-style-type: none"> • The background of the actions bar on a Grid View when items are selected • The background of parent and relationship components in a Parent and Child relationship tree
button-primary	<ul style="list-style-type: none"> • The background of buttons such as New and Action

Table 104. Color settings (continued)

Color setting	UI elements the setting applies to
button-primary-active	<ul style="list-style-type: none"> The object component in a Parent and Child relationship tree The background of buttons such as New and Action when clicked
button-primary-hover	The background of buttons such as New and Action when the mouse pointer hovers over them
button-tertiary	<ul style="list-style-type: none"> The outline and text of buttons on Task and Admin tabs The New Section button on the Design tab in the View Designer
button-tertiary-hover	The background of buttons on Task and Admin tabs when the mouse pointer hovers over them
button-tertiary-active	The background of buttons on Task and Admin tabs when clicked
focus	The outline of the UI element that currently has focus
interactive	<p>The fill style of check marks, for example in Grid Views</p> <p>The color of the loading spinner icon that is displayed when content is loading</p>
link-primary	<p>Text in clickable links:</p> <ul style="list-style-type: none"> The names in a Grid View list The name of the view following the title of an object in Grid View The more link in a description
link-primary-hover	<p>Text in some clickable links when the mouse pointer hovers over them, except the names in a Grid View list:</p> <ul style="list-style-type: none"> The name of the view following the title of an object in Grid View The more link in a description
text-on-color	Text in buttons, such as New and Action

Procedure

1. Click  > **Solution Configuration** > **Themes**.

2. Click **Add Theme**.

3. Select a theme in **Base Theme**.

The colors of the base theme are applied as a preview. Select a different base theme, if needed.

4. Enter a **Name**. Make it meaningful. It is displayed to users in the  > **Change Theme** task.

5. Enter a **Description**.

6. Leave **Enabled** cleared.

7. In **Colors** click a setting and apply a color by performing one of the following steps:

- Click a color on the color model.

- Click the drop down. The options depend on the browser you use. For example, for Chrome, there are options to provide color values as RGB, HSL, and HEX.
8. Repeat the previous step for each UI element.
9. Click **Done**.

What to do next

Test the theme, make adjustments as needed, and enable it. After the custom theme is enabled, it is available to users to apply.

Chapter 14. Views

Views control what information is displayed to users and how they interact with OpenPages.

When you configure the UI, you configure views that users access. You design the content and layout of a view by using the View Designer.

Prerequisite

Before you plan and design the views, learn about the components in the UI. For information, see *Navigating the UI* in the *IBM OpenPages with Watson User Guide*.

Show me how

This video provides an overview of views and the View Designer.

<https://youtu.be/R7ytoazgwg4>

Grid Views, Creation Views, Task Views, and Admin Views

The UI uses the following types of views:

- Grid Views
- Creation Views
- Task Views
- Admin Views

For each type of view, there can be:

- system views
- custom views

System views

System views are read-only views that are provided with OpenPages to get you started. You can use them as they are and as templates and learning tools for custom views that you create on your own.

For each object type, OpenPages provides at least one system Grid View, one system Creation View, and one or more system Task Views.

For a system view, you can:

- set the **View Priority**
- make it enabled
- make it disabled if you no longer use the view
- make it a default view

You cannot modify or delete a system view. However, you can create a custom view that is a copy of a system view. For more information, see [“Creating a custom view from a system view” on page 255](#).

For system views, in the View Designer you can view the **JSON** tab but the **Design** tab is hidden. To view a system view in the **Design** tab, copy it to a custom view and open the **Design** tab in the custom view.

Custom views

Custom views are views that you create on your own. You can create them for all object types and all view types.

For a custom view, you can:

- Customize the content of the view to your specific requirements
- Set the **View Priority**
- Make it enabled
- Make it disabled if you no longer use the view
- Make it a default view

For custom views, in the View Designer you can design the view on the **Design** tab. There is no need to use the **JSON** tab.

Controlling what views are displayed to users

You use rules on Grid Views, Creation Views, Task Views, and Admin Views to control what views are displayed to users. You can define one or more Grid Views, Creation Views, Task Views, and Admin Views for an object type.

For simplicity, the explanation below describes how to control what Creation Views are displayed to users. The same logic applies to Grid Views, Task Views, and Admin Views.

If you define one Creation View for an object type, you select **Use as default view for this object type for all profiles** on the view.

If you define multiple Creation Views for an object type, you define Creation Views where **Use as default view for this object type for all profiles** is cleared and rules determine what view is displayed to a user. You must still define one Creation View that is the default. For this view, you select **Use as default view for this object type for all profiles**.

Creation Views with rules take precedence over the default Creation View. The default Creation View is displayed if none of the Creation Views with rules match for a user after the rules have been checked.

View Priority on default views is always set to 1 and cannot be changed. **View Priority** on default views is disregarded during this selection.

Improve performance

To improve performance, use filters to limit the number of objects that are displayed in a view.

Grid Views

A Grid View shows a list of objects for a selected object type and allows you to filter, search, and select a specific object.

The screenshot shows a web-based application interface for 'IBM OpenPages with Watson'. At the top, there's a navigation bar with icons for Home, Controls, and other system functions. Below the navigation is a title bar 'Controls (83)' and a sub-titler '[View Name : SysView-Grid-SOXControl]'. The main area is a grid table with the following columns: Name, Description, Status, Classification, Design Effectiveness, and Operating Effectiveness. Each row represents a control object with a checkbox, a name like 'Control 12345', a detailed description, and status indicators such as 'Awaiting Assessment' or 'Key Control Activity'. The 'Design Effectiveness' and 'Operating Effectiveness' columns contain green circular buttons labeled 'Effective' or 'Not Determined'. A 'New +' button is located in the top right corner of the grid header.

Name	Description	Status	Classification	Design Effectiveness	Operating Effectiveness
Control 12345 Global Financial Services > North America > Retail Banking	Nulla sollicitudin lorem vel urna gravida, et feugiat libero venenatis. Maecenas eget sagittis more	Awaiting Assessment	Not Determined	Effective	Not Determined
Control 12346 Global Financial Services > North America > Retail Banking	Nulla sollicitudin lorem vel urna gravida, et feugiat libero venenatis. Maecenas eget sagittis more	Awaiting Assessment	Key Control Activity	Effective	Not Determined
Control 12347 Global Financial Services > North America > Retail Banking	Nulla sollicitudin lorem vel urna gravida, et feugiat libero venenatis. Maecenas eget sagittis more	Awaiting Assessment	Standard Control Activity	Effective	Not Determined
Control 12348 Global Financial Services > North America > Retail Banking	Nulla sollicitudin lorem vel urna gravida, et feugiat libero venenatis. Maecenas eget sagittis more	Awaiting Assessment	Not Determined	Effective	Not Determined
Control 12349 Global Financial Services > North America > Retail Banking	Nulla sollicitudin lorem vel urna gravida, et feugiat libero venenatis. Maecenas eget sagittis more	Awaiting Assessment	Standard Control Activity	Effective	Not Determined

Figure 23. Example of a Grid View

When you select an object type from the Primary menu, the dashboard, or a Task View, a Grid View is displayed.

In a Grid View, you can take the following actions:

- Select an object that you want to work with and open it.
- Click in the search box, enter free text, and press Enter. All objects that contain the text are returned.
- Click in the search box, enter specific values for enumerated fields, and press Enter. You can also build a list of selection criteria for multiple values and multiple fields.
- Click to access public and private filters.
- Clear the **Active Only** check box, if it is displayed, to show objects that are not in an active workflow. You can overwrite the **Active Only** filter or create your own default filters for object types that do not use workflows.
- Select one or more objects with the check mark and then you can delete, lock, unlock, move, and export them (depending on the object type and permissions).
- Select one or more objects with the check mark and then you can update field values by clicking **Bulk Update** (bulk update). The fields that allowed to be updated are configured in the view.
- Click a field name in the header row to sort the list by that field in ascending order. Click the field name again to choose descending order.
- Click **New +** to create a new object. Whether the icon is displayed depends on how your system is configured.
- Choose a value in **Items per page** to control how many objects are listed on a single page.

A Grid View lists objects for a single object type.

Grid Views for bulk workflow actions are Grid Views but with some differences in functionality due to their access point. For more information, see “[Defining Grid Views for bulk workflow actions](#)” on page 259.

Creation Views

A Creation View is used to define new objects.

The screenshot shows the IBM OpenPages with Watson interface. At the top, there's a navigation bar with icons for Home, Controls, and New Control. The main area is titled "Control" and "New Control". On the left, there's a "General" section with fields for "Name *", "Description *", and "Additional Description". Above these fields, there are "Required" and "Modified" status indicators. On the right, there's a sidebar with a message: "4 items require attention." followed by a list: "All Key Items (4) ▾", "Name *", "Description *", "Control Owner *", and "Risk *". At the bottom right are "Cancel" and "Save" buttons.

Figure 24. Example of a Creation View

A Creation View is displayed when you click **New** + from the dashboard, a Grid View, or a Task View. The icon might be named differently, depending on your configuration.

To use a Creation View, you complete the fields in the view and save the object. At a minimum, you must provide values in required fields.

A primary parent object is required for most object types. Depending on the access point and how the views are defined, the parent object can be defaulted or you might be required to provide one. For example, when you click **New** from a Grid View for Issues, you are required to provide a parent object such as a Control. From this access point the parent object is not known and you must provide it. However, if you are on a Task View for a Control and create a child Issue object, the parent object can be defaulted from the Task View and you must not select it.

Most Creation Views must provide a means for the selection of a primary parent since a parent object is required for most object types.

Creation Views for adding files (system and non-system) must provide a means to upload a file. For more information, see “[Defining Creation Views for file object types](#)” on page 264.

Task Views

A Task View is used to complete work that has been assigned to you.

The screenshot shows the IBM OpenPages with Watson interface with the title bar "IBM OpenPages with Watson". The top navigation bar includes "Home", "Controls", "New Control", "Issues", and a search bar "Policy nee...". Below the navigation is a toolbar with icons for "Issue", "Issue Status", "Priority" (set to "Low"), "Action Items" (0), "Cancel", and "Save".

The main content area displays a task titled "Policy needs update" with a star icon. It has two tabs: "Task" (selected) and "Activity". Under "Task", there is a "Reveal editable fields" toggle set to "Off". A "General" section contains fields for "Name" (marked as required) and "Description" (which includes a note about improving Watson suggestions). A "Controls" section shows buttons for "Select Primary Control", "Select Additional Controls", and a highlighted button "ISO Control Suggestions (1)". A message below says "There are no Controls".

On the right side, there is a sidebar with sections for "Issue In Progress" (status "In progress", due date "9/14/2020") and "Validation". The validation section has a red box around the "ISO Control Suggestions (1)" button and another red box around the "Issue Owner" field in the "Deficiency Details" section. It also shows a message "Select an action to validate" and a progress bar indicating "1 item requires attention". Other validation items listed include "Name", "Description", "Issue Category", "Issue Owner" (highlighted with a red box), "Issue Approver", "Priority", and "Due Date".

Figure 25. Example of a Task View

You open a Task View from the following access points:

- In a Grid View, you select an object and open it.
- In a report, you click an object and open it.
- In a Task View, you can open another Task View.

In a Task View, you can take the following actions:

- Review information about the object.
- Click ⓘ to view field guidance for fields in a section.

- Click the **Activity** tab to view change history.

- If it is displayed, click  to translate values in text fields to the language associated to your locale. For more information, see [“IBM Watson Language Translator” on page 847](#).

Depending on how the Task View is configured, you might also be able to take the following actions:

- Use the inline guidance and user guidance to help you understand what you need to do.
- Change information about the object.
- Associate the object to another object.
- Disassociate an object from another object.
- Create objects.
- Delete objects.
- If **Select an action to validate** is displayed in user guidance, you can check whether an action would pass validation before you complete the action.
- Choose an action, for example, Approve or Reject, to complete the task.
- Use Watson Moments to help you make object associations.
- Add a comment (reason) when you choose an action, if a comment window is displayed. The comment can be required or optional.
- View a tree structure that displays the object's relationship to other objects and navigate through the structure.
- View information about the object in a chart and navigate into the chart.
- View information about the object in a card or grid and navigate through to the objects in the card or grid.
- View cards, grids, charts, and trees that are organized in tab groups. For more information, see [“Organizing relationship fields in tab groups” on page 312](#).
- Add file attachments. For more information, see [“Defining Task Views for file object types” on page 269](#).
- Open and edit Microsoft Office files, if configured. For more information, see [“Defining Task Views for file object types” on page 269](#).

Admin Views

Use an Admin View to view and edit the field values and associations of an object. You can see an Admin View for an object only if you have the permission All Permissions/S0X/User Interfaces/View Admin tab.

Unlike a Task View, an Admin View shows all fields and relationships for the profile regardless of the stage in the object's lifecycle. You can manually add fields to an Admin View to ensure that the fields appear in the order you prefer. The order that you choose is also used when the fields are imported and exported. If you don't add the fields manually, the fields appear in a random order in the **Other fields** section of the Admin View and they are not imported or exported.

To open an Admin View, click an object in Grid View and click the **Admin** tab in the view.

The screenshot shows the Admin view for a Risk object named "RB-01-Risk00189". The top navigation bar includes icons for Home, Risks, and a specific document titled "RB-01-Risk...". The main content area has tabs for Task, Activity, and Admin, with Admin selected. A search bar and a "Reveal editable fields" toggle are at the top of the Admin section. The General tab contains fields for Name (RB-01-Risk00189), Description (Receipts are not properly authorized (authorization & approval)), Additional Description (Lorem Ipsum is simply dummy text of the printing and typesetting industry. Lorem Ipsum has been the industry's standard dummy text ever since the 1500s, when an [more](#) link is present), and Owner (ORM User). The Risk Categorization tab lists Risk Category (Clients, Products and Business Practices) and Risk Sub-Category (Improper Business or Market Practices). The Status and Approval tab shows Status (Awaiting Assessment) and Submit for Approval? (No). Other visible sections include Financial Statement Assertions, Domain, General Guidance, and Rejection Comment.

Figure 26. Example of an Admin View

From the **Admin** tab, you can take the following actions:

- Review information about the object.
- Select **Reveal editable fields** to view field values that can be edited and edit the values as needed.
- Change parent and child associations. For more information, see [“Associating objects by using Admin View” on page 254](#).
- If you want to view the change history, click the **Activity** tab. For more information, see [Viewing change history on the Activity tab in the IBM OpenPages with Watson User Guide](#).
- If you want to view more information about the object, click the **Task** tab. For more information, see [Completing work that is assigned to you in the IBM OpenPages with Watson User Guide](#).

Associating objects by using Admin View

You can associate objects using the **Parents** and **Children** sections of Admin Views. By default, parent and child relationships are automatically added to an Admin View at run time for object type relationships in the profile.

About this task

Depending on the object type, you might be able to link multiple parent or child objects to it. For example, a Risk object can have multiple parent objects, such as Control Objectives and Risk Assessments, child objects such as Controls and Issues, and files and links. Associations can be created or removed without affecting the related object or file.

Procedure

1. Click  to open the Primary menu.
2. Expand the categories to see the object types.
3. Select the object type that you want to work with.
A Grid View opens.
4. Click the name of the object that you want to work with.
5. Click the **Admin** tab.
If the **Admin** tab is not available, the Role Template that is associated with your user account does not have the necessary permission to view the tab.
6. If you want to add a parent, use the following steps:
 - a) In the **Parents** section, click the object type for the parent.
 - b) Click **Add**.
 - c) In the **Add** dialog box, select the objects that you want to add as parents and click **Done**.
7. If you want to make a parent the primary parent, use the following steps:
 - a) In the **Parents** section, click the object type for the primary parent.
 - b) Click **Set primary parent**.
 - c) In the **Set primary parent** dialog box, select the object that you want to be the primary parent and click **Done**.
If the object is not on the list of parents, it is added.
8. If you want to delete an object from the list of parents, use the following steps:
 - a) In the **Parents** section, select the object that you want removed from the list of parents.
 - b) Click **Remove**.
 - c) When prompted to confirm the removal of the object, click **Remove**.
If the object is not on the list of parents, it is added.
9. If you want to add a child, use the following steps:
 - a) In the **Children** section, click the object type for the child.
 - b) Click **Add**.
 - c) In the **Add** dialog box, select the objects that you want to add as children and click **Done**.
If you want to add a File object as a child, you can click **Add/Update** to choose a file from a browser window. For other object types, you can add a child by clicking **New** to create a new object.

10. If you want to create a new child, use the following steps:

- a) In the **Children** section, click the object type for the child.
- b) Click **New**.
- c) In the new tab, enter the required fields as necessary to create the new object.
- d) Click **Save** to create the new object.

When you create a new object in the **Children** section, its association with the parent object depends on the type of new object.

For example, if you create a new Control object from the Admin tab of a Risk object and the Create View for the Control object requires a different parent object type, an association between the Risk and Control will not occur. To enable the association, the administrator must modify the Create View of the Control object to permit the association.

Creating custom views

Determine what views you want to use for each object type.

Define the views by using the following methods:

- Use a system view as is.
- Make a copy of a system view and modify the copy to meet your requirements.
- Make a copy of a published custom view and modify the copy to meet your requirements.
- Define a view from scratch.

Creating a custom view from a system view

You can create a custom view by making a copy of a system or custom view and modifying the new view.

About this task

The source view and the new custom view must be for the same view type and the same object type, for example, both views must be task views for Issues.

Procedure

1. Click  > **Solution Configuration** > **Views**.
2. On the list of views, click **Include system views**.
3. Click **New View**.
4. Define information for the new view.
5. In **Copy from view (Optional)**, select the source view to copy from.
6. Enter a description.
7. Click **Create**.

The View Designer opens with the layout of the source view.

8. Make changes to the view as needed.

Creating custom Grid Views

Create a Grid View for a selected object type to list, filter, search, and select specific objects.

Designing a Grid View

A Grid View contains fixed and configurable UI components.

Controlling what Grid View is displayed to a user

An object type can have multiple Grid Views that are enabled. You define rules that determine what Grid View is displayed to a user. A Grid View can be displayed:

- For all or specific profiles.

For more information, see [“Controlling what views are displayed to users” on page 248](#) and [“Defining a Grid View” on page 257](#).

When users access an object type that does not have an enabled, valid Grid View, an error is displayed.

Designing a Grid View for scalability and performance

Consider scalability and performance when you design Grid Views. For example, if there are 500,000 Control objects in a library, a Grid View for Controls can be slow to display if no filters are applied.

For quicker system performance, apply a default filter to Grid Views that are defined for object types that potentially display a large number of objects.

For more information, see [“Defining default filters on Grid Views” on page 286](#).

Fixed UI components in a Grid View

Table 105. Fixed UI components in a Grid View	
UI component	Description
Work area	The work area (the grid) is always displayed.
Filter icon (🔍)	Is always displayed and cannot be hidden.
The name of the object type	Is always displayed and cannot be hidden.
The number of objects returned	Is always displayed and cannot be hidden.
The Search box	Is always displayed and cannot be hidden.
New button	Is displayed if creation is allowed at the object level and per the user's access permissions.
Checkboxes next to objects	Are always displayed and cannot be hidden.
The word <i>more</i>	Is always displayed when text is longer than can be shown. It cannot be hidden.
Items per page	Is always displayed and cannot be hidden.

Configurable UI components in a Grid View

Table 106. Configurable UI components in a Grid View	
UI component	Description
Work area	The work area (the grid) consists of columns and rows. You can configure how many columns are displayed and what fields display in each column. The header row in the grid is always displayed. The content of the rows is determined by the data that the user filters.

Table 106. Configurable UI components in a Grid View (continued)

UI component	Description
Display alternate field labels	<p>You can change the locale to display alternate field labels. For information, see “Applying alternate field labels” on page 285.</p>
Default filter	<p>If the object type has workflows, the Active Only check box displays. You can optionally overwrite the Active Only filter. If the object type does not have workflows, you can create your own default filter.</p> <p>For information, see “Defining default filters on Grid Views” on page 286.</p>
New button	<p>Is displayed if creation is allowed for the object type and the user has access permissions for the object type.</p>
The  (Bulk Update) icon	<p>Is displayed if registry settings that control bulk update functionality are configured for the user and object type. For more information, see:</p> <ul style="list-style-type: none"> • “Disable Bulk Update link” on page 496 • “Exclude object types from bulk updates” on page 496 • “Hide the Bulk Update feature for user profiles” on page 496 <p>The fields that are allowed to be updated are configured by the Bulk update setting in the view definition. Fields that are not displayed in the Grid View can also be updated, if configured.</p> <p>Bulk update is not available for read only fields, for example, computed fields, workflow fields, and system fields that are read only.</p> <p>Administrators with the Bulk Update All Fields application permission can bypass the restrictions on fields that can be updated. For more information, see “Types of application permissions” on page 52.</p>
Defining colors for enumerated field values	<p>You can add colors to values in enumerated field values. For more information about how to apply colors to field values, see “Defining enumerated string fields” on page 170.</p>
Applying color ranges	<p>You can apply colors to value ranges for decimal, integer, and currency data types. For more information about how to apply colors to field value ranges, see “Defining fields and adding them to field groups” on page 161.</p>

Defining a Grid View

A Grid View definition contains basic information and rules. When used, a Grid View shows a list of objects for a selected object type that you can filter, search, select a specific object, and perform bulk updates on multiple objects.

Before you begin

Plan and design the Grid Views. For more information, see “[Designing a Grid View](#)” on page 256.

If you define multiple Grid Views for an object type, see “[Controlling what views are displayed to users](#)” on page 248.

Turn on the **Display debug info** feature. For more information, see “[Displaying debug information](#)” on page 277.

About this task

Each object type can have one or more Grid Views that are enabled.

For quicker system performance, apply a default filter to Grid Views that are defined for object types that potentially display a large number of objects.

Procedure

1. Click  > **Solution Configuration** > **Views**.
2. Click **New View**.
3. Leave **Enabled** selected.
4. Select **Use as default view for this object type for all profiles** to make the view the default task view for the object type.
5. Select an object type in **Object type**.
6. Enter a **Name**. Allowed characters are A-Z, a-z, 0-9, underscore, hyphen, and spaces. Special characters are not allowed.
7. Select **Grid** in **View Type**.
8. Select a source view in **Copy from view (Optional)** to start with a base view that you can then modify. Choose a system Grid View or a published custom Grid View.

If you do not select a view, the new view is empty (minimum properties). You must design a new view.
9. Enter a **Description**.

If you select **Use as default view for this object type for all profiles**, click **Create** to create the view. Otherwise, you can click **Rules** and specify the criteria that determines the Creation View that is displayed to a user.
10. Set **View Priority** to a numeric value, such as 0, 1, or 2. It establishes the display priority of a Grid View compared to other Grid Views for the same object type. If multiple Grid Views match for a user after the rules have been checked, **View Priority** determines the view that is displayed to the user. For example, a Grid View with the lowest value 0 is displayed first, then 1, then 2.
11. Optional: In **Profiles (if not specified, view is valid for all profiles)**, select one or more profiles.
12. Click **Create**.

The View Designer opens with the **Design** tab displayed.
13. Design the view.
 - a) Set the **Bulk update** toggle to allow a field to be updated when a user clicks **Bulk Update**.
 - b) Add the fields to the **Fields enabled for bulk update but not in grid view** section. Fields that are listed in this section are not displayed in the Grid View but users can update them when they click **Bulk Update**.

For more information, see “[Using the View Designer](#)” on page 272.
14. Click **Preview** to see how the view appears to a user.
15. Click **Publish**.
16. Test the view. Every time that you change the view, you need to publish it and retest it.

What to do next

If you need to change the rules after a view is saved, click .

Defining Grid Views for bulk workflow actions

Grid Views for bulk workflow actions are designed to optimized speed and efficiently as users work on actions created by GRC Workflow.

Before you begin

Understand the bulk workflow actions feature in GRC Workflow and determine whether it is needed.

Determine whether unique Grid Views are needed for the feature. Any Grid View can be used for bulk workflow actions. The reason to create unique Grid Views for bulk workflow actions is to customize the columns to meet the needs of the users completing the tasks.

About this task

A Grid View for bulk workflow actions is displayed when a user accesses tasks from the **Complete task with bulk workflow actions** window.

In the following example, a user selected to work with tasks assigned to them by the RCSA workflow, which is displayed in Workflow Name in the header. The stage is displayed next to the workflow name. In this example, the user has 43 risk assessments to review. The options in the toolbar, Approve, Reject, and Return, come from the workflow stage.

The screenshot shows a web-based application window titled "IBM OpenPages with Watson". At the top left is a navigation bar with icons for home, search, and user profile. A dropdown menu is open, showing "Bulk Action" with a red box around it. To the right of the menu are icons for notifications, settings, and user profile. Below the menu, the title "Bulk Workflow Action (43)" is displayed, with "43" in blue, followed by a "Unsaved Filter" button and a "Workflow Name: RCSA" field showing "Stage (Status): In Review" with a red box around it. A large blue header bar contains the text "43 items selected" and several buttons: "Approve", "Reject", "Return", "Bulk Update" with a pencil icon, and "Cancel". Below this is a table with the following data:

Name	Description	Stage (Status)	Risk Category	Inherent Risk Rating	Residual Risk Rating	Action
Risk Assessment 1	Risk	In Review	Client, Product	Low	Low	<input type="checkbox"/>
Risk Assessment 2	Risk	In Review	Execution	Low	Low	<input type="checkbox"/>
Risk Assessment 3	Risk	In Review	Execution	Low	Low	<input type="checkbox"/>
Risk Assessment 5	Risk	In Review	Execution	Low	Low	<input type="checkbox"/>
Risk Assessment 7	Risk	In Review	Client, Product	Low	Low	<input type="checkbox"/>
Risk Assessment 11	Risk	In Review	Client, Product	Low	Low	<input type="checkbox"/>

Figure 27. Example of a Grid View for bulk workflow actions

Functionality between a Grid View and Grid View for bulk workflow actions is mostly the same except for these differences:

- The Grid View that is displayed is defined in the workflow stage.
- The options in the toolbar are defined in the workflow stage. They cannot be configured in the View Designer.
- The **New** button is hidden.
- The tab name is always **Bulk Action**.
- The Grid View head is always Bulk Workflow Action.

Procedure

1. Follow the instructions in [“Defining a Grid View” on page 257](#) to define a Grid View.
2. Add fields. The fields will be columns in the Grid View. Choose columns that will be helpful to the user when they work with bulk workflow actions.

3. Click **Done**.

What to do next

Add the Grid View to the workflow. Open the workflow and go to the **Bulk Workflow Action** section.

Select the Grid View in **Select a grid view for Bulk Workflow Action**. For more information, see “[Defining a standard stage](#)” on page 397.

Creating custom Creation Views

Create a Creation View to define new objects.

Designing a Creation View

A Creation View contains fixed and configurable UI components.

Controlling what Creation View is displayed to a user

An object type can have multiple Creation Views that are enabled. You define rules that determine what Creation View is displayed to a user. A Creation View can be displayed:

- For all or specific profiles.
- For one or more parent object types if the parent object is known.
- For any parent object types if the parent object is known.

Most Creation Views must provide a means for the creation of a primary parent since a parent object is required for most object types. The access point determines how the parent object can be provided:

- For Creation Views that are accessed by clicking **New** from a Grid View, the parent object is not known and the view must contain a relationship field that allows a user to select a parent object.
- For Creation Views that are accessed from a relationship field in a Task View, the parent object is known since the object is open. The view need not contain a relationship field that allows a user to select a parent object. For these Creation views, if you did not select **Use as default view for this object type for all profiles**, you can use the **Rules** tab to define a rule and set **Parent Types (if known at creation time)** to specific parent object types or select **Any** for any parent object types.

Use this feature in Creation Views for two reasons:

- So that users do not need to select a parent object. This makes the view easier to use because selecting objects is time consuming and unnecessary because the parent object is known.
- So that different Creation Views can be displayed based on the parent object type. For example, a Creation View for an Issue can be different depending on whether it is accessed from a parent object that is a Control versus an Asset.

For more information, see “[Controlling what views are displayed to users](#)” on page 248 and “[Defining a Creation View](#)” on page 263.

When users access an object type that does not have an enabled, valid Creation View, no view is displayed.

Associating a primary parent object and parent/child objects

For most object types, a Creation View must provide the ability to associate a primary parent object.

You can add a card or grid relationship field with an **Add** action to a Creation View. When a user adds the first object, that object is automatically set as the primary parent.

If you want ensure that a specific object type is set as the parent, set the **Required** property on the relationship field to True to make the field mandatory.

To have a Creation View take over the parent object from the access point where the user starts, define a rule for the Creation View by setting **Parent Types (if known at creation time)** on the **Rules** tab. You can

set **Parent Types (if known at creation time)** to specific parent object types or select **Any** for any parent object types.

Creation Views might also provide the ability to associate one or more parent objects. To do this, add a card or grid relationship field with an **Add** action to a Creation View.

If a Creation View allows users to associate both a primary parent object and parent objects, you can define one relationship field with two actions, **Set Primary Parent** and **Add**. You can make the relationship field required but you cannot ensure that a user provides a primary parent object. If the user does not explicitly choose a primary parent, the first object that was added as a parent becomes the primary parent when the object is saved.

You can use rules on relationship fields to help a user select the correct associations. You can use the visible and hidden rules on a relationship field to show or hide a relationship field based on the value of another field in the view. For example, if you create an Issue, the issue type that the user chooses can determine the parent object type that is displayed.

For more information about relationship fields, see [“Adding and configuring relationship fields on views” on page 290](#).

Creation Views for adding files

Creation Views for adding files (system and non-system) must provide a means to upload a file. For more information, see [“Defining Creation Views for file object types” on page 264](#).

Fixed UI components in a Creation View

Table 107. Fixed UI components in a Creation View	
UI component	Description
Work area	The work area is always displayed.
	The Save icon is always displayed and cannot be hidden. It is clickable after all required information for an object has been entered.
	The Cancel icon is always displayed and cannot be hidden.
Object type and New [object type]	The name of the object type is always displayed in the header.
	Field guidance for each section is displayed if at least one field in the section is defined with a field description.
	The search icon is always displayed. Use it to search for fields in the view.

Configurable UI components of a Creation View

Table 108. Configurable UI components in a Creation View	
UI component	Description
Work area	You configure the content of the work area by defining sections and adding fields to each section.
Inline guidance	You can add inline guidance. For information, see “Adding inline guidance” on page 280 .

Table 108. Configurable UI components in a Creation View (continued)

UI component	Description
User guidance	<p>You can add user guidance that includes information text and a list of key fields.</p> <p>For information, see “Adding user guidance” on page 282.</p>
Adding fields to sections	<p>Fields are organized in sections.</p> <p>For information, see “Adding a section” on page 278.</p>
Organizing fields into columns	<p>You can organize fields in columns.</p> <p>For information, see “Arranging fields in columns” on page 280.</p>
Defining colors for enumerated field values	<p>You can add colors to values in enumerated field values.</p> <p>For more information about how to apply colors to field values, see “Defining enumerated string fields” on page 170.</p>
Applying color ranges	<p>You can apply colors to value ranges for decimal, integer, and currency data types.</p> <p>For more information about how to apply colors to field value ranges, see “Defining fields and adding them to field groups” on page 161.</p>
Displaying alternate field labels	<p>You can change the locale to display alternate field labels.</p> <p>For information, see “Applying alternate field labels” on page 285.</p>
Associating objects	<p>You can add the ability to associate objects, for example, associate a primary parent to a new object.</p> <p>For information, see “Adding a card layout” on page 292 and “Adding a grid layout” on page 304.</p>
Organizing relationship fields in tab groups.	<p>“Organizing relationship fields in tab groups” on page 312</p>
Accessing a natural language processing service	<p>You can provide the ability to make suggestions by using a natural language processing service.</p> <p>For information, see “Adding a classifier field that makes taxonomy suggestions” on page 288.</p> <p>For information, see “Adding a classifier field that makes object association suggestions” on page 309</p>
Adding URL links	<p>You can add URL fields that display as buttons or links.</p> <p>For information, see “Displaying a URL launcher field as a button or link” on page 287.</p>
Uploading files	<p>You can add the ability to upload files to Creation Views for file object types.</p> <p>For information, see “Defining Creation Views for file object types” on page 264.</p>

Defining a Creation View

A Creation View definition contains basic information and rules. When used, a Creation View enables a user to define new objects.

Before you begin

Plan and design the Creation Views. For more information, see “[Designing a Creation View](#)” on page 260.

If you define multiple Creation Views for an object type, see “[Controlling what views are displayed to users](#)” on page 248.

If you define Creation Views for file object types, see “[Defining Creation Views for file object types](#)” on page 264.

Turn on the **Display debug info** feature. For more information, see “[Displaying debug information](#)” on page 277.

About this task

Each object type can have one or more Creation Views that are enabled.

Procedure

1. Click  > **Solution Configuration** > **Views**.
2. Click **New View**.
3. Leave **Enabled** selected.
4. Select **Use as default view for this object type for all profiles** to make the view the default Creation View for the object type.
5. Select an object type in **Object type**.
Do not choose File in **Object type**. To create files, use a relationship field. For more information, see “[Defining Task Views for file object types](#)” on page 269.
6. Enter a **Name**. Allowed characters are A-Z, a-z, 0-9, underscore, hyphen, and spaces. Special characters are not allowed.
7. Select **Creation** in **Type**.
8. Select a source view in **Copy from view (Optional)** to start with a base view that you can then modify. Choose a system Creation View or a published custom Creation View.
If you leave **Copy from view (Optional)** blank, the new view is empty (minimum properties). You must design a new view.
9. Enter a **Description**.
If you select **Use as default view for this object type for all profiles**, click **Create** to create the view. Otherwise, you can click **Rules** and specify the criteria that determines the Creation View that is displayed to a user.
10. Click **Rules**.
11. Set **View Priority** to a numeric value, such as 0, 1, or 2. It establishes the display priority of a Creation View compared to other Creation Views for the same object type. If multiple Creation Views match for a user after the profile and parent object type rules have been checked, **View Priority** determines the view that is displayed to the user.
For example, a Creation View with the lowest value 0 is displayed first, then 1, then 2.
12. Optional: In **Profiles (if not specified, view is valid for all profiles)** select one or more profiles.
13. Optional: In **Parent Types (if known at creation time)**, select one or more specific parent object types or **Any**.

If you use this rule, ensure that you also have a default view. A default view can be used if the parent object type is different than the selected object types or if the parent object type is unknown at

creation time. Examples of instances where the parent object type is unknown include when you click **Add** from a Grid View or dashboard widget.

14. Click **Create**.

The View Designer opens with the **Design** tab displayed.

15. Design the view.

A Creation View must, at a minimum, contain a name. Depending on the object type, you might need to add a primary parent. You can add a primary parent by using a card or grid relationship field that contains an action to associate a parent. For more information, see [“Adding actions to relationship fields” on page 313](#).

For more information, see [“Using the View Designer” on page 272](#).

16. Click **Preview** to see how the view appears to a user.

17. Click **Publish**.

18. Test the view. Every time that you change the view, you need to publish it and retest it.

What to do next

If you need to change the rules after a view is saved, click .

Defining Creation Views for file object types

Creation Views are used to add files to the OpenPages file repository.

About this task

A Creation View for the File (SOXDocument) object type is used when users create new files from the following access points:

- A Task View that contains a grid relationship field for files. In this case, the parent object for the file is the object type of the Task View, for example, a Control or an Issue.

A **Files to add** window is shown after you select a file but before you click **Upload**. Creation Views for files determine the fields that are displayed in the **Files to add** pop-up window. Only required fields are displayed in the **Files to add** window.

- The  > **Attachments** > **Files** task. In this case, the parent object for the file is a business entity that the user provides. A **Files to add** window is not displayed.

When you plan Task Views that contain grid relationship fields for files, review the system Creation View for the File object type. You can use it as or create custom views if needed. It might be valuable to use multiple Creation Views for files so that you can control what displays in the **Files to add** pop-up window. You can define one Creation View for files and use it for all parent object types. Alternatively, define multiple Creation Views for files and use rules to control which Creation View for files is applied based on parent object type. Use the **Parent Types (if not specified, view is valid for all parent types)** rule on Creation Views to control what fields display in **Files to add**. For example, files that are added to a Policy object can include fields that support the Policy Import trigger. However, files that are uploaded to all other object types can exclude these fields. For more information, see [“Designing a Creation View” on page 260](#).

Creation Views are also used when users create files from the  > **Attachments** > **Files** task.

Creation Views are also used when administrators create new system files from the  > **System Configuration** > **System Files** task. System Creation Views are provided for the objects types for system files.

Procedure

1. Follow the instructions in [“Defining a Creation View” on page 263](#) to define a Creation View.

2. Select File in **Object type** (or one of the system file object types).
3. Add fields to the Creation View.
4. Drag a **File Uploader** element to a section. This element allows you to select a file to upload. It is unique to Creation Views for files. It is required.
5. Add a grid relationship field that contains an action to associate a parent. For more information, see [“Adding actions to relationship fields” on page 313](#). This is not applicable to Creation Views for system files.
6. Click **Done**.

Creating custom Task Views

Create a Task View so that a user can use it to complete the work assigned to them.

Designing a Task View

A Task View contains fixed and configurable UI components.

Controlling what Task View is displayed to a user

An object type can have multiple Task Views that are enabled. You define rules that determine what Task View is displayed to a user. A Task View can be displayed:

- For all or specific profiles.
- If the value of an enumeration field on an object is a specific value.
- If the signed on user matches the value of a user field, for example, is the owner or assignee.

For more information, see [“Controlling what views are displayed to users” on page 248](#) and [“Defining a Task View” on page 268](#).

When users access an object type that does not have an enabled, valid Task View, no view is displayed.

Task Views for adding and managing files

Task Views are used to support adding and managing files. For more information, see [“Defining Task Views for file object types” on page 269](#).

Fixed UI components in a Task View

Table 109. Fixed UI components of a Task View	
UI component	Description
Task View header	A Task View header is always displayed. The object type and object name are always displayed in the Task View header and cannot be hidden.
Work area	The work area is always displayed.
Activity tab	The Activity tab is displayed if a user has the Audit Trail application permission.
ⓘ	Field guidance for each section is displayed if at least one field in the section is defined with a field description.
🔍	The search icon is always displayed. Use it to search for fields in the view.

Table 109. Fixed UI components of a Task View (continued)

UI component	Description
Icons for IBM Watson Language Translator	If IBM Watson Language Translator has been configured for the current object type and the signed on user has the Watson Language Translator UI permission, the  icon displays in Task Views. It displays regardless of whether there is text that can be translated. The icon requires no configuration in Task Views. For more information, see “IBM Watson Language Translator” on page 847.

Configurable UI components in a Task View

Table 110. Configurable UI components of a task view

UI component	Description
Task View header	You can configure fields and the Actions button in the Task View header. For information, see “Defining a Task View header” on page 284.
Work area	You configure the content of the work area by defining sections and adding fields to each section.
Inline guidance	You can add inline guidance. For information, see “Adding inline guidance” on page 280.
User guidance	You can add user guidance that includes information text, a list of key items, and the ability to validate actions. For information, see “Adding user guidance” on page 282.
Adding fields to sections	Fields are organized in sections. For information, see “Adding a section” on page 278.
Organizing fields into columns	You can organize fields in columns. For information, see “Arranging fields in columns” on page 280.
Defining colors for enumerated field values	You can add colors to values in enumerated field values. For more information about how to apply colors to field values, see “Defining enumerated string fields” on page 170.
Applying color ranges	You can apply colors to value ranges for decimal, integer, and currency data types. For more information about how to apply colors to field value ranges, see “Defining fields and adding them to field groups” on page 161.
Displaying alternate field labels	You can change the locale to display alternate field labels. For information, see “Applying alternate field labels” on page 285.

Table 110. Configurable UI components of a task view (continued)

UI component	Description
Reviewing and associating related objects	<p>You can add the ability to review and associate related objects, for example, a primary parent or child objects.</p> <p>For information, see “Adding a card layout” on page 292 and “Adding a grid layout” on page 304.</p>
Applying dynamic filters when associating related objects	<p>You can apply dynamic filters when associating related objects using a card or grid relationship field.</p> <p>For information, see “Defining dynamic filters on actions in relationship fields” on page 317.</p>
Adding new objects	<p>You can provide the ability to add new objects.</p> <p>For information, see “Adding actions to relationship fields” on page 313.</p>
Copying objects	<p>You can provide the ability to copy objects.</p> <p>For information, see “Adding actions to relationship fields” on page 313.</p>
Adding files (attachments)	<p>You can add the ability to add files (attachments).</p> <p>For information, see:</p> <ul style="list-style-type: none"> • “Defining Task Views for file object types” on page 269 • “Defining Creation Views for file object types” on page 264
Delete objects	<p>You can provide the ability to delete child objects.</p> <p>For information, see “Adding a Delete action” on page 317.</p>
Adding tree diagrams to display object relationships	<p>You can display object relationships in a tree diagram.</p> <p>For information, see “Adding a tree diagram” on page 307.</p>
Adding charts to display object relationships	<p>You can display object relationships in a chart diagram.</p> <p>For information, see “Adding a chart diagram” on page 294.</p>
Displaying related objects as a count	<p>You can display related objects as a count.</p> <p>For information, see “Adding a count” on page 303.</p>
Organizing relationship fields in tab groups.	<p>“Organizing relationship fields in tab groups” on page 312</p>
Accessing a natural language processing service	<p>You can provide the ability to make suggestions using a natural language processing service.</p> <p>For information, see “Adding a classifier field that makes taxonomy suggestions” on page 288 and “Adding a classifier field that makes object association suggestions” on page 309.</p>
Adding URL links	<p>You can add URL fields that display as buttons or links.</p> <p>For information, see “Displaying a URL launcher field as a button or link” on page 287.</p>

Defining a Task View

A Task View definition contains basic information and rules. When used, a Task View enables a user to complete work that is assigned to them.

Before you begin

Plan and design the Task Views. For more information, see [“Designing a Task View” on page 265](#).

If you define multiple Task Views for an object type, see [“Controlling what views are displayed to users” on page 248](#).

If you define Task Views that allow users to add file attachments, see [“Defining Task Views for file object types” on page 269](#).

Turn on the **Display debug info** feature. For more information, see [“Displaying debug information” on page 277](#).

About this task

Each object type can have one or more Task Views that are enabled.

Custom views can be edited. System views open in read-only mode and the **Design** tab is hidden.

Procedure

1. Click  > **Solution Configuration** > **Views**.
2. Click **New View**.
3. Leave **Enabled** selected.
4. Select **Use as default view for this object type for all profiles** to make the view the default task view for the object type.
5. Select an object type in **Object type**.
6. Enter a **Name**. Allowed characters are A-Z, a-z, 0-9, underscore, hyphen, and spaces. Special characters are not allowed.
7. Select **Task** in **View Type**.
8. Select a source view in **Copy from view (Optional)** to start with a base view that you can then modify. Choose a system Task View or a published custom Task View.
If you do not select a view to copy from, the new view is empty (minimum properties). You must design a new view.
9. Enter a **Description**.
If you select **Use as default view for this object type for all profiles**, click **Create** to create the view. Otherwise, you can click **Rules** and specify the criteria that determines the Task View that is displayed to a user.
10. Set **View Priority** to a numeric value, such as 0, 1, or 2. It establishes the display priority of a Task View compared to other Task Views for the same object type. If multiple Task Views match for a user after the profile, enumeration, and user rules have been checked, **View Priority** determines the view that is displayed to the user.
For example, a Task View with the lowest value 0 is displayed first, then 1, then 2.
11. Set **Rule Operator** to one of the following options:
 - **Logical AND of all rules**
All of the rules (profile, enumeration rules, and user rules) must be met for the view to be shown to a user.
 - **Logical OR of all rules**
Any one of the rules (profile, enumeration rules, and user rules) must be met for the view to be shown to a user.

12. Optional: In **Profiles (if not specified, view is valid for all profiles)** select one or more profiles.
13. In **Enumeration rule**, you can set a view to display if the value of an enumeration field on the object is a specific value.
 - a) In **Rule Field**, select the field that the rule is based on.
 - b) In **Rule Condition**, select the condition.
For example, select equal (=) or not equal to (<>).
 - c) In **Rule Value**, select the value that the rule tests against.
14. In **User rule**, you can set a view to display if the signed on user has the role of the value that is selected.
For example, is the owner or assignee of the object.
 - a) In **Rule Field**, select the field that the rule is based on.
For example, select assignee or <object> owner.
 - b) Click  to add more user rules.
15. Click **Create**.
The View Designer opens with the **Design** tab displayed.
16. Design the view. For more information, see [“Using the View Designer” on page 272](#).
17. Click **Preview** to review the view.
18. Click **Publish**.
19. Test the view. Every time that you change the view or the rules, you need to publish it and retest it.

What to do next

If you need to change the rules after a view is saved, click .

Defining Task Views for file object types

To support adding and managing files (attachments) in Task Views, define a Task View for the File (SOXDocument) object type.

Before you begin

Complete the following prerequisites:

- Define Task Views for object types, for example, Controls and Issues, that allow file attachments. Add a grid relationship field where **Object Type** is set to File and **Relationship Type** is set to children. The **Add/Update** button automatically displays in a grid relationship field. It is used to upload new files to the selected object. If you add an Association action, users can also associate files that are already uploaded to other objects. They can also disassociate files by selecting a row and clicking **Remove**.
- Review the Creation Views for the File (SOXDocument) object type. A Creation View for files is required to add file attachments in a Task View. Use the system view for the File object type as is or create custom views. For more information, see [“Defining Creation Views for file object types” on page 264](#).
- Configure whether Microsoft Office documents can be opened and edited directly from OpenPages. For more information, see [“Enabling and configuring the opening of Microsoft Office files” on page 488](#).

About this task

In the following example, a Task View for Audit objects contains a grid relationship field for files. An Audit object is open and you can upload a file by clicking **Add/Update** or dragging a file to the Task View. You can also click **Associate action** to associate an existing file to the object and **Remove** to disassociate objects.

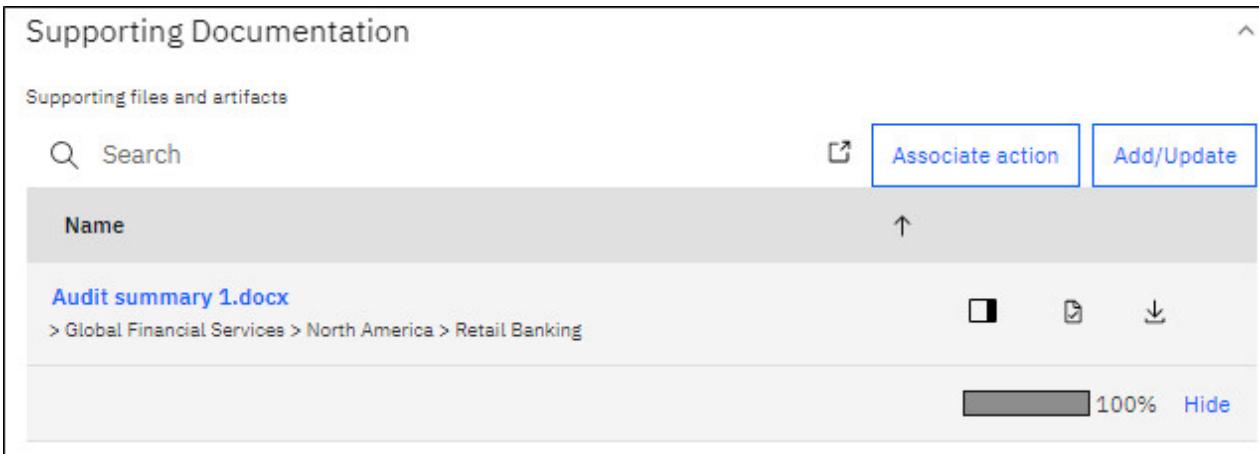


Figure 28. Example of a Task View for files

For more information about relationship fields, see [“Adding a grid layout” on page 304](#).

In addition to having a relationship field for files in a Task View, you must also define Task Views for the File object type. When you click a file name in a grid relationship field for files, the Task View for the File object type opens.

Define one Task View for the File object type and use it for all parent object types. Alternatively, define multiple Task Views for the File object type and use rules to control which Task View for files is displayed for each parent object type.

OpenPages uses version control and file locking in the file repository. When you work in a collaborative team environment, files are checked in and out to ensure that changes made by one team member will not be overwritten by another team member.

Version management and the ability to check in and check out files are always enabled. The check in and check out icons require no configuration. You can, however, control whether a **Versions** element in a Task View for files is displayed. It allows you to view and work with multiple versions of a file.

In this example, the Task View for the Files object type is defined with File Name, Description, Document Type, Folder, Active, Last Modification Date, and a Versions element.

The screenshot shows a 'Task View' for a file named 'Audit summary 1.docx'. The 'General' section contains fields for Name (Audit summary 1.docx), Description, Created By (System Administrator - OpenPagesAdministrator), Last Modified By (System Administrator - OpenPagesAdministrator), Creation Date (Mar 31, 2020 12:31:57 PM GMT), Last Modification Date (Mar 31, 2020 12:31:57 PM GMT), and Folder (/ Global Financial Services / North America / Retail Banking). Below this is a 'Versions' section with a table header: Last Modification Date, Last Modified By, Comment. A single row is shown: Mar 31, 2020 12:31:57 PM GMT, System Administrator - OpenPagesAdministrator, and a comment icon.

Figure 29. Example of a Task View for files

Task Views are also used when users view files from the **Attachments > Files** task.

Task Views are also used when administrators view system files from the **System Configuration > System Files** task. System Task Views are provided for the objects types for system files.

Procedure

1. Follow the instructions in “Defining a Task View” on page 268 to define a Task View.
2. Select File in **Object type** (or one of the system file object types).
3. Add fields to the Task View.
4. Drag a **Versions** element to a section. This element allows you to view and manage multiple versions of a file. It is unique to Task Views for files.
 - a) Apply rules to the Versions element (optional). For more information, see “Configuring rules” on page 318.
 - b) Click **Done**.
5. Click **Done**.

Creating custom Admin Views

Create an Admin View to view and edit the field values and associations of an object.

Defining an Admin View

An Admin View definition contains information about an object that an administrator can view and edit.

Before you begin

Determine the Admin Views you need.

If you define multiple Admin Views for an object type, see “Controlling what views are displayed to users” on page 248.

About this task

Each object type can have one or more Admin Views that are enabled.

Custom views can be edited. System views open in read-only mode and the **Design** tab is hidden.

Procedure

1. Click  > **Solution Configuration** > **Views**.
2. Click **New View**.
3. Leave **Enabled** selected.
4. Select **Use as default view for this object type for all profiles** to make the view the default admin view for the object type.
5. Select an object type in **Object type**.
6. Enter a **Name**. Allowed characters are A-Z, a-z, 0-9, underscore, hyphen, and spaces. Special characters are not allowed.
7. Select **Admin** in **View Type**.
8. Select a source view in **Copy from view (Optional)** to start with a base view that you can then modify. Choose a system Admin View or a published custom Admin View.
If you do not select a view to copy from, the new view is empty (minimum properties). You must design a new view.
9. Enter a **Description**.
If you selected **Use as default view for this object type for all profiles**, click **Create** to create the view. Otherwise, you can click **Rules** and specify the criteria that determines the Admin View that is displayed to a user.
10. Set **View Priority** to a numeric value, such as 0, 1, or 2. It establishes the display priority of an Admin View compared to other Admin Views for the same object type. If multiple Admin Views match for a user after the profile, enumeration, and user rules have been checked, **View Priority** determines the view that is displayed to the user.
For example, an Admin View with the lowest value 0 is displayed first, then 1, then 2.
11. Optional: In **Profiles (if not specified, view is valid for all profiles)**, select one or more profiles.
12. Click **Create**.
The View Designer opens with the **Design** tab displayed.
13. Design the view. For more information, see [“Using the View Designer” on page 272](#).
14. Click **Preview** to review the view.
15. Click **Publish**.
16. Test the view. Every time that you change the view or the rules, you must publish and retest it.

What to do next

If you need to change the rules after a view is saved, click .

Using the View Designer

Use the View Designer to define, publish, and manage views.

To open the View Designer, click  > **Solution Configuration** > **Views**. Your access permissions determine whether the menu item is displayed.

The View List is displayed.

View List

The View List shows the views that are defined. From the View List, you can:

- Click a view. The View Designer opens and you can view or make changes to the view.
- Filter the View List by typing in the **Search** box.
- Filter the View List by object type and view type by using the **Filter by** boxes.
- Select **Include system views** to show system views in the View List. The setting is cleared by default. Custom views are always listed.
- Click a column header to change the sort order of the list.
- Select the check box next to a single view or multiple views to update numerous views. The bulk update options are:
 - Delete
 - Enable
 - Disable
 Clear the check boxes to hide the bulk update options.
- Click **New View** to create a new view. After you define the initial properties, the View Designer opens. For more information, see:
 - [“Defining a Grid View” on page 257](#)
 - [“Defining a Creation View” on page 263](#)
 - [“Defining a Task View” on page 268](#)
 - [“Defining an Admin View” on page 271](#)

The View Designer

The View Designer has the following components:

- **Design** tab
- **JSON** tab
- **Preview** tab

Design tab

The **Design** tab shows the definition of the view in a graphical format. It has the following components:

- Canvas

The canvas is where you lay out the view, create sections, and add fields to sections.

- Palette

UI components on the palette allow you to add inline guidance, groups, relationship fields, object fields, and workflow fields to a view. Use **Hide fields already in view** to control whether fields that are already added to the view are displayed in the palette.

- Property panel

The content of the property panel changes depending on what you select on the canvas. It can be properties that apply to a field or to a UI component (relationship field, group, inline guidance, and so on).

The following example shows the components on the **Design** tab:

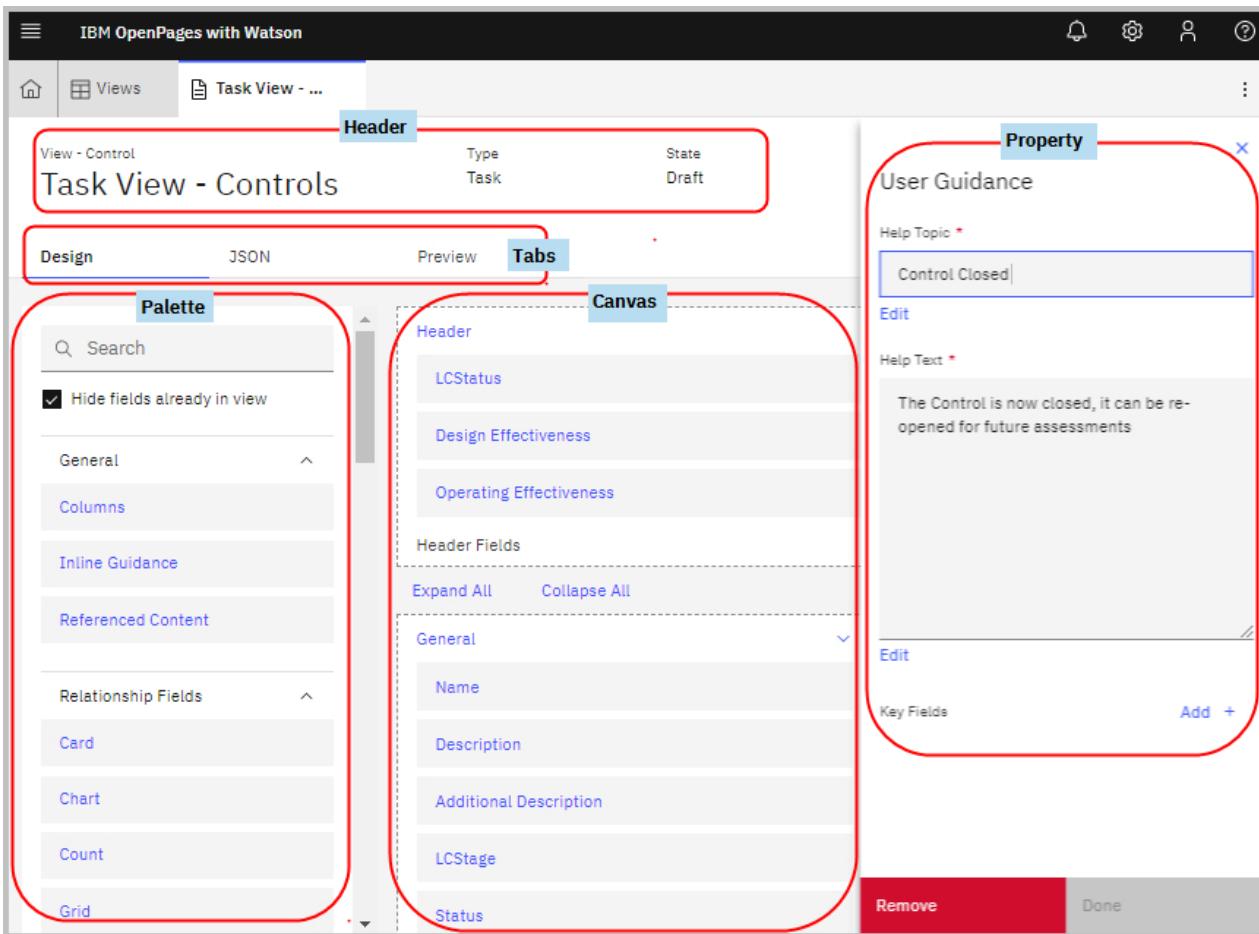


Figure 30. The Design tab in the View Designer

The **Design** tab is hidden for system views.

JSON tab

The **JSON** tab shows a view definition as JSON code.

The following example shows the JSON code for the previous task view definition.

The screenshot shows the 'Task View - Controls' view in the View Designer. The top navigation bar includes 'IBM OpenPages with Watson', 'Views', 'Task View - ...', and a menu icon. Below the navigation is a toolbar with 'View - Control', 'Type Task', 'State Draft', 'Discard Draft', and 'Publish'. The main area has tabs for 'Design', 'JSON' (which is selected), and 'Preview'. The JSON code is displayed in a code editor:

```
1 - {
2 -   "guidance": {
3 -     "nameLabels": [],
4 -     "helpTopicLabels": [],
5 -     "helpTextLabels": [],
6 -     "fields": []
7 -   },
8 -   "nameLabels": [],
9 -   "header": {
10 -     "fields": [],
11 -     "actionFields": []
12 -   },
13 -   "sections": [
14 -     {
15 -       "name": "General",
16 -       "nameLabels": [
17 -         {
18 -           "locale": "it_IT",
19 -           "value": "General"
20 -         },
21 -         {
22 -           "locale": "en_GB",
23 -           "value": "General"
24 -         },
25 -       ]
26 -     }
27 -   ]
28 - }
```

Figure 31. The JSON tab in the View Designer

For more information about JSON, see [“Editing JSON for a view definition” on page 277](#).

Preview tab

The **Preview** tab shows a view definition for an object instance. Up to 50 objects are displayed. Filters are disabled. Objects are read-only and cannot be changed. Workflow stages and workflow stage overrides are not considered. You cannot use the Preview tab to test how a view appears at different stages in a workflow and whether workflow task overrides are functioning correctly.

The following example shows the **Preview** tab for the previous task view definition.

The screenshot shows the 'Task View - Controls' page in the View Designer. At the top, there are tabs for 'Design', 'JSON', and 'Preview'. The 'Preview' tab is selected. Below the tabs, there's a large input field labeled 'Choose Control' with 'RCM CTL 101.1' listed. The main area is titled 'Control' and shows 'RCM CTL 101.1' with a star icon. It has two tabs: 'Task' (selected) and 'Activity'. Under 'Task', there's a checkbox for 'Edit Mode' and a note about required and modified fields. The 'General' section contains fields for 'Name' (Required), 'Description' (with a link to 'Review original supporting documentation'), 'Additional Description' (with a note about authorization), and 'Status' (set to 'Awaiting Assessment').

Figure 32. The Preview tab in the View Designer

Automatically translating labels

If it is configured, the “IBM Watson Language Translator” on page 847 can help you define labels in multiple languages. There are numerous access points in the View Designer.

If it is displayed, click to populate translated values to languages. For more information, see “IBM Watson Language Translator” on page 847.

Saving a view

Your work is automatically saved as you edit a view. A general syntax validation check is performed every time that a view is saved.

Publishing a view

Click **Publish** when the view is finished. A detailed validation check is performed every time that a view is published. This validation check is more in depth than the one performed by the auto-save. It looks at whether the view is suitable for use and crosschecks the entire view. If you receive an error when you publish a view, you need to resolve it.

Discarding a draft version of a view

To discard changes you made to a view, click **Discard Draft**. All changes since the last published version are discarded.

Disabling a view

To disable a view, select the view in the View list, and then click **Disable**.

Alternatively, click the **Edit** icon for a view, and then clear the **Enabled** check box.

Working on a view as a team

When you have a view open in the View Designer, the URL contains the view's internal name. If you are working on the view with colleagues, you can send them the URL to share your progress. Although you can collaborate with colleagues, only one user should work on a view in the View Designer at a time.

Displaying debug information

Use **Display debug info** to turn on debug mode and resolve problems as you configure views.

About this task

When **Display debug info** is enabled, the following additional elements are displayed in the header when you access views:

- The name of the view that is open.

When the view name is shown, you can test the view rules and verify that the correct view is displayed. Click the view name, and the View Designer opens.

- **Why can't I save?**

Why can't I save? is displayed in Creation, Task, and Admin Views if there's a problem that prevents you from saving your work. For example, if a required field for an object is empty, the **Save** button is disabled. Click **Why can't I save?** to view informational text that explains why **Save** is not enabled.

Procedure

1. Click  > **Other** > **Display Debug Info**.

Debug mode is turned on and a check mark displays next to **Display Debug Info**.

2. To turn off debug mode, click **Display debug info** again.

Debug mode is turned off and the check mark is removed.

Editing JSON for a view definition

The content and layout of views is defined in JSON, which is syntax for defining structured data.

When to use the JSON tab

Use the **JSON** tab to copy views. For more information, see [“Creating a custom view from a system view” on page 255](#).

Other than copying views, there is no need to use the **JSON** tab. You can optionally check how a view is structured and search for JSON property and element names. You can solely use the **Design** tab to create and design custom views. All the capabilities in the **JSON** tab are also in the **Design** tab.

Tips for fixing JSON mistakes

The JSON editor checks syntax and shows mistakes.

- The mistake is usually in the line just before the line with a red x.
- Check first for mismatched delimiters (curly braces and square brackets) and trailing commas. They are the most common mistakes. The error message might not clearly state that the problem is a delimiter.

Tips for copying JSON and minimizing copy errors

Avoid errors by copying an entire view rather than JSON snippets.

If you copy a JSON snippet, use the small triangles in the left gutter to collapse the JSON before you select a JSON snippet. When the text is collapsed, it is easier for you to select what you want to copy.

Before you paste a JSON snippet, collapse the area that you are pasting into so that it is easier to identify the correct insertion point.

Adding general elements to a view

You can control a view's fundamental content and organization.

Adding a section

Information in a view definition is organized into sections.

About this task

Sections are valid in Creation, Task, and Admin Views.

A section contains fields and inline guidance. When you work on the **Design** tab:

- You can add a section. When you add a section, it appears as the last section.
- You can control the order of sections in a view.
- You can define whether a section is collapsed or expanded when a user initially opens a view.
- You can expand and collapse individual sections or all sections using the **Expand All** and **Collapse All** toggles.
- You cannot embed a section in another section.
- You can add fields directly to sections, in which case they are ordered consecutively down the page in the view.
- You can add groups to sections and then add fields to groups, in which case you can arrange the fields in columns and place them more precisely in the view.
- If a Task View is used in a workflow, task view overrides can hide a section and override the **Initially Collapsed** setting. For more information, see “[Defining a standard stage](#)” on page 397.

In an Admin View, sections can either be dynamic, which means the fields are automatically added at run time, or static. Creation and Task Views contain only static sections. An Admin View can contain the following dynamic sections:

- The **Other fields** section contains fields that are in the profile but not already in the view. Fields in **Other fields** are not imported or exported by FastMap. If you want a field to be exported or imported, add the field to a nondynamic section.
- The **Parents** section automatically displays grid fields for all enabled parent relationship types.
- The **Children** section automatically displays grid fields for all enabled child relationship types.
- The **Parent and child relationships** section displays a relationship tree with parents and children.

On the JSON tab, a section is defined in a `sections` element.

Procedure

1. In the View Designer, click the **Design** tab.

The palette is displayed.

2. If the view is an Admin View and you want to add a dynamic section, click **New Dynamic Section** and select the type of dynamic section you want to add.
If all of the dynamic sections are already in the view, you can't add a new dynamic section and **New Dynamic Section** is not displayed.
3. If you want to add a static section, click **New Section**.
4. Enter a **Label** for the section. Click **Edit** to enter localized values.

If it is displayed, click  to populate translated values to languages. For more information, see “IBM Watson Language Translator” on page 847.

5. Set **Initially Collapsed** to **True** or **False**.
6. Click **Done**.
7. Expand the new section and start adding fields and groups.
 - a) To add a field directly to the section, drag it into **Section Fields**.
 - You can drag a field either from the palette or the canvas and drop it into the section.
 - You can change the order of fields in a section.
 - b) To add groups, see “Arranging fields in columns” on page 280.
8. Optional: Drag an **Inline Guidance** element from the palette to the section. For more information, see “Adding inline guidance” on page 280.
9. Click **Done**.
10. Move the section up or down to change the display order.

Adding a trend chart based on field value change history

You can add a trend chart with fields to a Task or Admin View to display the trends of numeric fields over time.

You can select the time period, the fields that you want displayed in the chart, and the colors to represent the trend for each field.

The chart shows data from the currently selected reporting period only. If the time period you select for the chart doesn't overlap with the current reporting period, the chart is empty.

All dynamic date ranges are based on the current date, regardless of selected reporting period.

Procedure

1. In the View Designer, click the **Design** tab.
The palette is displayed.
2. Perform one of the following actions:
 - a) From the list of **General** items in the palette, drag **Trend Chart (fields)** into any existing section labeled **Section Fields**.
 - b) Click **New Section** to create a new section in the view. From the list of **General** items in the palette, drag **Trend Chart (fields)** into the new section.
For more information about creating new sections, see “Adding a section” on page 278.
3. In the **Trend Chart (fields)** panel, enter a **Label**. Click **Edit** to enter localized values.
4. To edit the **Trend Chart Fields Configuration**, click **Edit**.
5. Select a **Time period** for the trend chart.
You can select one of the following options:
 - **Static range** to choose a **Start date** and **End date**.

- A dynamic date range that specifies a number of months: 1, 3, 6, 12, or 24 months. A dynamic date range uses the current date as the end date of the range.
 - **All time.**
6. Select the **Trend fields** that you want to see in the trend chart.
 7. Select the **Chart colors** for each field in the trend chart.
 8. Click **Done** to finish configuring the trend chart fields. Click **Done** to finish adding the trend chart.
 9. If you have completed your changes in the View Designer, click **Publish**.

Arranging fields in columns

You can use columns (groups) to control field placement in a view.

About this task

Columns are valid in Creation Views and Task Views.

When you work on the **Design** tab:

- A group must be within a section.
- Groups can contain object fields and relationship fields.
- A group cannot be embedded in another group.

If multiple columns are defined but horizontal space is limited, the display changes to a single column.

You can find an example in: SysView-Task-SOXControl.

On the JSON tab, columns are defined in a `columns` property.

Procedure

1. In the View Designer, click the **Design** tab.
The palette is displayed.
2. Drag a **Column** element from the palette to the section where you want it to display.
3. Enter a value in **Name**. This is an internal name that is not displayed in the view.
4. Select a number in **Number of Columns**. You can define no more than four columns.
5. Click **Done**.
6. Add fields to the group. You can drag a field either from the palette or the canvas and drop it into **Group Fields**.
There is no limit on the number of fields you can have in a column.
7. Move fields up or down to change the display order.

Adding inline guidance

Inline guidance displays customer-specific help text that supports users as they complete a task. It is displayed as a field and enclosed in a box.

About this task

Inline guidance is valid in Creation Views and Task Views.

Each section can contain one or more inline guidance elements.

Visible or hidden rules can be applied to each field within an inline guidance section.

When it is displayed in a view, users can expand or collapse the text if it is long.

IBM OpenPages with Watson

Workflows Issue Review Business Ent... + *New Loss E...

New Loss Event

Cancel Save

* Required * Modified ⓘ

General ⓘ

Name *

_LE_0002

*Description *

Stolen customer data

*Owner *

orm

Search users

*Outcome

Loss

*What Happened

A missing security patch allowed hackers to enter the server hosting the online banking system. System was brought down for several hours while the problem was corrected.

Inline guidance

Please provide correction information based on the information provided by the responsible parties.

The screenshot shows the 'New Loss Event' form in the IBM OpenPages with Watson application. The 'General' section includes fields for Name (value: '_LE_0002'), Description (value: 'Stolen customer data'), Owner (value: 'orm'), Outcome (value: 'Loss'), and What Happened (value: 'A missing security patch allowed hackers to enter the server hosting the online banking system. System was brought down for several hours while the problem was corrected.'). An 'Inline guidance' callout box is highlighted with a red border, containing the text: 'Please provide correction information based on the information provided by the responsible parties.'

Figure 33. Example of inline guidance

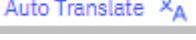
On the JSON tab, inline help is defined in `helpTopic` and `helpText` properties.

Procedure

1. In the View Designer, click the **Design** tab.
The palette is displayed.
2. Drag an **Inline Guidance** element from the palette to a section.
3. Enter a value in **Name**. This is an internal name that is not displayed in the view.
4. Enter text in **Help Topic**. This value is displayed in bold as a header. Click **Edit** to enter localized values.

If it is displayed, click  to populate translated values to languages. For more information, see “IBM Watson Language Translator” on page 847.

5. Enter text in **Help Text**. This value is the informational text to which you can optionally apply formatting. Click **Edit** to enter localized values.

If it is displayed, click  to populate translated values to languages. For more information, see “IBM Watson Language Translator” on page 847.

6. Add a hidden or visible rule (optional). For information, see “Defining Visible and Hidden rules” on page 320.
7. Optional: Apply formatting. For more information, see “Applying light formatting to text” on page 283.
8. Click **Done**.

Adding user guidance

User guidance supports users as they complete a task and resolve issues.

About this task

User guidance is valid in Creation Views and Task Views.

User guidance is displayed in a panel in the upper right corner of a view. It contains informational text, a progress bar, and a list of key items. If a task is part of a workflow that has started, **Select an action to validate** is also displayed. Messages and field symbols guide users through finishing a task.

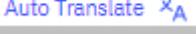
When it is displayed in a view, users can expand or collapse the text if it is long.

A view can have one user guidance section. The name *user guidance* is shown in the View Designer but the section has no title when it is displayed in a view.

For more information about user guidance, see “How key items and workflow actions display in user guidance” on page 283.

Procedure

1. In the View Designer, click the **Design** tab.
The palette is displayed.
2. Click **User Guidance**. The User Guidance panel opens.
3. Enter text in **Help Topic**. This value is displayed in bold as a header. Click **Edit** to enter localized values.

If it is displayed, click  to populate translated values to languages. For more information, see “IBM Watson Language Translator” on page 847.

4. Enter text in **Help Text**. This value is the informational text to which you can optionally apply formatting. Click **Edit** to enter localized values.

If it is displayed, click  to populate translated values to languages. For more information, see “IBM Watson Language Translator” on page 847.

5. Build the list of key fields. There are two methods. For object fields, you can follow this method:
 - a) In the User Guidance panel, click **Add**. A list of object fields is displayed.
 - b) Tick the fields that you want to include as key fields.
 - c) Move key items up and down to change the display order.
 - d) Click **Done**. The User Guidance panel closes. The panel changes to a list of key fields.

For object fields and any other fields, for example, relationship fields, that are on the canvas, follow this method:

- a) Close the User Guidance panel if it is open.
- b) Drag fields from the canvas to the list of key fields. A field can be dropped when the list of key fields is framed with a blue box. If the field does not drop, it is already marked as a key field.
- c) Move key items up and down to change the display order.

You do not have to add required fields as key items. However, if you add them, you can control the display order.

6. Optional: Apply formatting. For more information, see [“Applying light formatting to text” on page 283](#).

How key items and workflow actions display in user guidance

You can configure key items and how they are ordered in user guidance.

Key items in user guidance

Key items are listed after the informational text under the title **Key Items**. You configure the list of key items. In addition, required fields and invalid fields are automatically listed as key items. When a user clicks a key item, the cursor moves to that field and places it in edit mode. The symbols next to a field indicate its status. The symbols are fixed and cannot be changed.

Workflow actions and user guidance

If a task is part of a workflow that has started, **Select an action to validate** is displayed in the user guidance panel.

For more information about defining validations on actions, see [“Defining a workflow action” on page 407](#).

The workflow information card appears above the user guidance and contains summary information.

Neither **Select an action to validate** nor the workflow information card requires configuration.

Task view overrides can change the user guidance and key items that are displayed. For information, see [“Defining a standard stage” on page 397](#).

See the *IBM OpenPages with Watson User Guide* for more information about how users work with the user guidance panel.

Applying light formatting to text

You can apply light formatting to text in inline guidance, user guidance, and object text for field guidance.

About this task

HTML and line breaks are not supported.

Procedure

1. Access a task where you can define text, for example, defining inline guidance for a Task View in the View Designer.
2. Apply the following formatting to text:
 - To apply italics, enclose text in single asterisks, for example, *text*.
 - To apply bold, enclose text in double asterisks, for example, **text**.
 - To insert a hyperlink, provide a fully qualified URL. For example, <https://www.ibm.com> displays in a view as a hyperlink named <https://www.ibm.com>.
 - To insert a hyperlink as a link title, provide it in the [Link title] (URL) format. For example, <https://www.ibm.com> displays in a view as a hyperlink named <https://www.ibm.com>.
 - To begin a new paragraph, press enter twice.
 - To format text as a bulleted item, enter - (hyphen followed by one space and text) or * (asterisk followed by one space and text).

- To apply a heading level one, begin the text with # followed by a space, for example, # This is a Heading One. Use ## for heading level two, and so on. The maximum is six heading levels.
3. Alternatively, for inline guidance and user guidance on the JSON tab:
- Press enter to begin a new line (indented).
 - \n* (\n* followed by one space and text) formats text as a bulleted item.
 - \n\n begins a new paragraph.

Defining a Task View header

A Task View header contains object information and, optionally, an **Actions** button and fields.

About this task

A task view header is valid only in Task Views.

You can add an **Actions** button and up to three fields to a Task View header, where the field type can be integer, decimal, currency, simple text, enumerated, user, date, and relationship count. The Task View header has limited space so add fields whose content is short and concise.

If the object type has workflows, the workflow drives the options on the **Actions** button. For information, see [“How users interact with workflows” on page 373](#).

The options on the **Actions** button can be configured to allow a user to enter a comment. The comment can be required or optional. For information, see [“Defining a workflow action” on page 407](#).

If the object type does not have workflows, you can add one **Actions** button. The actions facilitate moving the object to the next stage in its lifecycle. The values are from any set of enumerated field values or from the configurable lifecycle transitions for the object. The field type must be enumerated. The label of the **Actions** button is fixed and cannot be changed.

You cannot add rules to fields in the Task View header.

In this example, the Task View header for the Issue object contains three fields: Issue Status, Priority, and Action Items.

Figure 34. Example of a Task View header for issues

You can find an example in: SysView-Task-SOXIssue.

On the JSON tab, a task view header is defined in a *header* element.

Procedure

1. In the View Designer, click the **Design** tab.
The palette is displayed.
2. Expand the **Header** panel.
3. In **Lifecycle Action**, choose an enumerated field that drives the **Actions** button.
4. Add fields to the header. You can drag a field either from the palette or the canvas and drop it into the group.

Applying alternate field labels

You can apply alternate field labels to support localization.

About this task

Alternate field labels are valid in Grid Views, Creation Views, and Task Views.

You can apply labels to fields and UI components in the UI that do not have localized text. The names of sections, inline guidances, and relationship fields are unique to the UI and have no localized text until you create it. For example, a section that is titled Remediation in English has no translated string in German. When you add the German title, a string key is automatically created.

For information about localization, see [Chapter 18, “Localizing text,” on page 443](#).

You can provide localized text only for labels where an **Edit** button is displayed.

On the JSON tab, localized values are defined in nameLabels properties for fields and UI components.

Procedure

1. In the View Designer, click the **Design** tab.
The palette is displayed.
2. Select the UI component, for example, a relationship field or a section.
3. Enter a value in the label. The value you entered is populated to all languages.
4. Click **Edit**.
5. Enter localized text for one or more languages.

If it is displayed, click  to populate translated values to languages. For more information, see “IBM Watson Language Translator” on page 847.

6. Click **Done**.

Results

String keys are automatically created for the localized text you add. If values change in the future, repeat the steps and make the changes.

Defining default filters on Grid Views

You can add default filter rules to a Grid View.

About this task

If you define a default filter, a check box with the label you provide displays at the top of the grid. It is selected by default. Only objects that match the filter are displayed in a view.

For quicker system performance, apply a default filter to Grid Views that are defined for object types that potentially display a large number of objects.

Filters can be based only on single value enumerated fields. A Grid View can have only one default filter but it can have multiple rules. An object must meet all rules to match the filter.

Grid Views for object types that have workflows display a filter named **Active Only**. If you define a default filter rule for an object type that has workflows, it overwrites the **Active Only** filter.

An example of a default filter is that you want a Grid View for SOXRisk objects to display only objects whose Status field is set to Approved. A check box labeled **Only display approved items** is displayed at the top of the grid.

You can use a filter so that a Grid View for SOXRisk objects displays only objects whose Status field is set to Reject and whose Audit Inherent Impact is 1 or 2. One check box labeled **Only display rejected items** is displayed at the top of the grid.

For more information about rules, see “Configuring rules” on page 318.

On the JSON tab, default filter rules are defined in a *defaultFilterRules* element in a Grid View.

Procedure

1. In the View Designer, click the **Design** tab.
The palette is displayed.
2. On the canvas, click **Define default filter**.
3. Specify a **Label**. This name displays at the top of the grid.
4. Click **New Rule**.
5. In **Field**, choose the field that the filter is based on. Only single value enumerated fields are listed.

6. In **Matches any of**, select the value or values that you want to filter on. If you add multiple values, an object must have one of the values to match the filter.
7. Click **Done**.
8. Add more rules, if needed. If you add multiple rules, an object must meet all rules to match the filter.
9. Click **Create**.

What to do next

Publish the Grid View to test the filter. Filters are not supported on the **Preview** tab.

Adding and configuring fields on views

You can add different kinds of fields to views and control how they are displayed.

Displaying a URL launcher field as a button or link

You can configure a URL launcher field to display as a button or link.

About this task

The property that controls how a URL launcher field is displayed is valid in Creation Views and Task Views.

URL launcher fields can be configured as a button or link. Whereas, URL fields always display as links.

Display Type is not shown in the property panel for URL fields.

For more information about URL launcher fields, see [“Using object fields to launch JavaServer Pages and external URLs” on page 188](#).

On the JSON tab, display type is defined by setting *subDisplayType* to `button` or `link`. The field's display type must be set to `URL`. If *subDisplayType* is not provided, the URL field displays as a link.

Procedure

1. In the View Designer, click the **Design** tab.
The palette is displayed.
2. Click a URL launcher field.
3. In the properties panel, set **Display Type** to **Button** or **Link**.

Displaying a number field as a progress bar

You can display a number field as a progress bar. Valid in Grid Views, Creation Views, and Task Views.

About this task

You can configure a number field to display as a progress bar. The field must be an integer or decimal, and it must have a minimum and maximum value that is defined at the field level.

For information about defining color ranges, see [“Colors for field value ranges” on page 158](#).

On the JSON tab, a progress bar is defined by setting *subDisplayType* to `Progress` for a number field.

Procedure

1. In the View Designer, click the **Design** tab.
The palette is displayed.
2. Click the field that you want to display as a progress bar.
3. In the properties panel, set **Display Type** to **Progress**.
4. Click **Done**.

Adding a classifier field that makes taxonomy suggestions

You can add classifier fields that make taxonomy suggestions using a natural language processing service.

Before you begin

The natural language processing service must already be configured to make taxonomy suggestions. Find out the classifier fields and classifier target fields before you get started. For information, see [“Natural language processing services” on page 850](#).

About this task

Classifier fields that make taxonomy suggestions are valid in Creation Views and Task Views.

The UI supports making taxonomy suggestions and object association suggestions. For information about object association suggestions, see [“Adding a classifier field that makes object association suggestions” on page 309](#).

When a user accesses a Creation View or Task View with a classifier field, an IBM Watson Insights button appears in place of the classifier field. The button name changes to the classifier field label. Click the button and an IBM Watson Insights panel displays the results.

The classifier field and the classifier input field must both be in the view. The classifier target fields can optionally be included in the view. It is not necessary to configure the Watson statement on the classifier input field (*Adding a description improves IBM Watson Suggestions*), the IBM Watson Insights button, or the IBM Watson Insights panel. These elements display automatically for classifier fields.

The classifier field label is used as both the button label and the title of the IBM Watson Insights panel. Otherwise, they cannot be customized.

You can add multiple classifier fields to a view.

You cannot add classifier fields that make taxonomy suggestions to Grid Views. You can, however, add classifier target fields to Grid Views.

In this example, the text in the Description is used as input to a natural language processing service that makes taxonomy suggestions. The loss event categorization field is configured to be a classifier field.

The screenshot shows the 'IBM OpenPages with Watson' interface. In the center, there's a 'New Loss Event' form. On the left, under 'General' settings, the 'Name' field is set to '_LE_0083' and the 'Description' field contains the text 'iphone not configured per policy'. Below this, the 'Owner' field is set to 'Search users'. Under 'Loss Event Categorization', there's a section titled 'Basel Category Suggestion (2)'. To the right, a sidebar titled 'Learn about IBM Watson insights' displays two suggestions. The first suggestion, 'Basel Category Suggestion', is for 'Employment Practices and Workplace Safety' with a relevant score of 31%. The second suggestion is for 'Execution, Delivery and Process Management' with a relevant score of 11%.

Figure 35. Example of a Classifier field that makes taxonomy suggestions

On the JSON tab, no properties are needed for taxonomy classifier fields.

Procedure

1. In the View Designer, click the **Design** tab.
The palette is displayed.
2. Drag the classifier input field either from the palette or the canvas and add it to a section or group.
3. Drag the classifier field either from the palette or the canvas and add it to a section or group. It is this field that is replaced with an IBM Watson Insights button.
Although it might make sense to place the two fields near each other, they can be in different groups or sections.
4. Click **Done**.

Adding a business entity selector field

A business entity selector field enables users to quickly identify the role a business entity plays.

Before you begin

The business entity selector field must already be configured. For more information, see [“Defining business entity selector fields” on page 165](#).

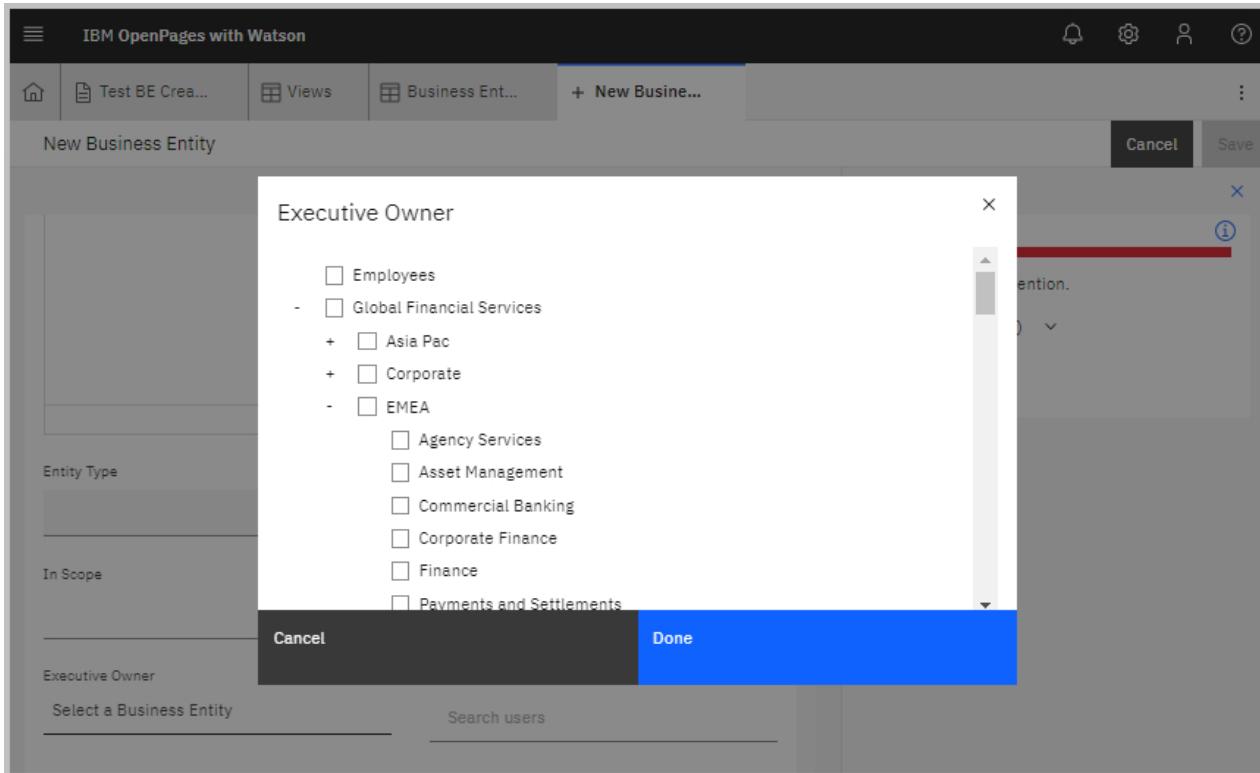
About this task

Business entity selector fields can be added to Grid Views, Creation Views, and Tasks Views.

Business entity selector fields can be added as key fields in user guidance.

In GRC Workflow, business entity selector fields can be used in task view override fields. They can also be used in conditions and validations. The options are Empty or Not empty.

The following example shows how a business entity selector field is rendered in a Creation View.



Procedure

1. In the View Designer, click the **Design** tab.
The palette is displayed.
2. On the canvas, drag a field that is defined as a business entity selector field to the canvas. The field attribute panel opens.
3. Set **Read Only** to true or false.
4. Set **Required** to true or false.
5. Add rules (optional). For more information, see [“Configuring rules” on page 318](#).
6. Click **Done**.
7. Publish the view.

Adding and configuring relationship fields on views

You can use relationship fields to support actions and render an object's associations to other objects in various graphical formats.

You can add the following types of relationship fields to views:

- Card
- Chart

- Count
- Grid
- Tree

You can apply rules to a relationship field, add actions to it, and control the related objects that are displayed within it.

Controlling whether a relationship field is visible, hidden, editable, read only, or required

You can apply **Rules** to all types of relationship fields. Rules allow you to more precisely control whether a relationship field is visible or hidden. For cards and grids, you can use rules to control some aspects of what users can do with related objects. For information, see [“Adding rules to relationship fields” on page 311](#).

Adding actions to a relationship field

You can add actions to cards and grids. You use an action, for example, to add, copy, or associate objects. For example, in a Task View for a Risk object, you might want to use an action that can associate a Control object to the object that is open in the view. For more information, see [“Adding actions to relationship fields” on page 313](#).

Controlling the objects that are displayed in a relationship field

The **Relationship Type** property controls the objects included in a relationship field based on the relationship between two object types: the object type for the view and the object type given in a relationship field.

The **Relationship Type** property exists on all types of relationship fields. Depending on the object type, it can be set to the following values:

- Children
- Parents
- Ancestors
- Descendants
- Siblings

The **Object Type** property controls the objects included in a relationship field based on the object type given in a relationship field. The **Object Type** property exists on all types of relationship fields except tree and all relationship types except siblings.

A sibling relationship type is to another object type that has the same parent. The allowed path is up to a parent object type and down to any other object type below that parent. For example, in a view for Controls, a relationship field can show other Controls that have the same parent Risk. A relationship field for a sibling relationship type has no **Object Type** property, instead it has **Parent Object Type** and **Sibling Object Type** properties. Sibling relationship type can be used in all relationship fields except trees. The sibling relationship type does not support actions.

You can apply the following filters to further restrict the objects that are included in a relationship field:

- You can apply a **Public Filter** to all types of relationship fields (card, chart, count, grid, or tree) and to any relationship type (Children, Parents, Ancestors, or Descendants). You use **Public Filter** to restrict the objects in a relationship field to those that meet the criteria of the specified public filter. If **Public Filter** is hidden in the property panel, no public filters for the object type exist.

For information about how to define a public filter for an object type, see [“Adding filters to object types” on page 208](#).

- You can apply a **Relationship Path** to a card, chart, count, or grid. You use **Relationship Path** to restrict the objects in a relationship field if the relationship type is Ancestors or Descendants.

If you provide multiple filters, the filters are combined with an AND statement. An object must match all the filters to be included in the relationship field.

Organizing relationship fields in tab groups

Use tab groups to maximize the use of space and improve usability. For more information, see [“Organizing relationship fields in tab groups” on page 312](#).

Adding a card layout

Use a card layout to display text-based information about a series of objects and make viewing and comparing multiple objects easy. It can also be used to add parent and child objects and select objects to work on.

About this task

Card layouts are valid in Creation, Task, and Admin Views.

A card layout shows related objects in boxes and supports actions. It is suited, for example, for displaying related regulations or parent business entities.

Use a card layout when only a few objects, for example, less than five, are expected to be displayed. Use a grid layout if you expect numerous objects to be displayed.

The **Fields** property controls the fields that are displayed in the relationship field. You can control what field the information is sorted by and the sort order.

If you choose an actor field in **Sort By**, the values are sorted by username (not first name and last name). The sort is case-sensitive.

In the following example, a business entity is open and each card shows a child business entity.

The screenshot shows the IBM OpenPages with Watson interface. At the top, there's a navigation bar with icons for Home, Business Ent..., Views, CustomView..., and High Oaks B... (which is currently selected). Below the navigation bar, the title "High Oaks Bank" is displayed with a dropdown arrow, a star icon, and a refresh symbol. The main content area has tabs for Task, Activity, and Admin, with Task being the active tab. Under the Task tab, there's a section titled "Associations" with a "Children" sub-section. Two cards are visible: one for "Africa and Middle East" and one for "Asia". Each card has a header, a "Description" field, a "Creation Date" field (showing "Feb 28, 2022 5:37:12 AM GMT"), and a "Created By" field (showing "System Administrator - OpenPagesAdministrator@openpages.local"). A blue-bordered "Add" button is located in the top right corner of the "Associations" section.

Figure 36. Example of a card layout

On the JSON tab, a card layout is defined with `type` as `relationship` and `subDisplayType` as `card`.

Procedure

1. In the View Designer, click the **Design** tab.
The palette is displayed.
2. Drag a Card element from the palette and add it to a section.
3. Enter a **Label**. It displays as a field header within a section. Click **Edit** to enter localized values.

If it is displayed, click **Auto Translate** to populate translated values to languages. For more information, see “IBM Watson Language Translator” on page 847.

4. Choose an option in **Relationship Type**:
 - Children
 - Parents
 - Descendants
 - Ancestors
 - Siblings
5. Choose an **Object Type** (displays for all relationship types except siblings). The objects that are listed vary depending on what you chose in **Relationship Type**.
6. Choose a **Parent Object Type** and a **Sibling Object Type** (displays only if **Relationship Type** is Siblings).

7. Complete the remaining fields. The fields that are listed vary depending on what you chose in **Relationship Type**.
8. Select a **Public Filter**, if one exists for the object type (optional).
9. Click **Add Action** to display an action button in the card (displays only if **Relationship Type** is Children or Parents).

If **Relationship Type** is Children, you can add the following types of actions:

- Add
- Copy Recursive
- Delete
- New
- Watson Suggestions

If **Relationship Type** is Parents, you can add the following types of actions:

- Add
- Set Primary Parent
- Watson Suggestions

For information about actions, see [“Adding actions to relationship fields” on page 313](#).

10. Choose a **Relationship Paths** (displays only if **Relationship Type** is Ancestors or Descendants).
11. Add **Fields** to the relationship field.
12. Choose a field in **Sort By**.
13. Define the **Sort Direction**.
14. Add rules to the relationship field (optional). For information, see [“Adding rules to relationship fields” on page 311](#).
15. Click **Done**.

What to do next

Place the card in a tab group (optional). For more information, see [“Organizing relationship fields in tab groups” on page 312](#).

Adding a chart diagram

Use a chart diagram when you want to view related objects in a graphic format based on a specific field.

About this task

Chart diagrams are valid in Task Views.

A chart is based on one object type and one field within that object type that is a single value enumerated field.

You can drill through the chart and open related objects.

The **Relationship Type** property controls the object relationships that are included in the chart diagram.

The following chart types are supported:

- Bar
- Doughnut
- Gantt
- Heat map (count-based and zone-based)
- Horizontal bar
- Pie

- Trend

For examples, see “[Chart diagram examples](#)” on page 296.

Note: Workflow fields are currently not supported in charts.

Procedure

1. In the View Designer, click the **Design** tab.
The palette is displayed.
2. Drag a Chart element from the palette and add it to a group or a section.
3. Enter a **Label**. It displays as a field header within a section. Click **Edit** to enter localized values.

If it is displayed, click  to populate translated values to languages. For more information, see “[IBM Watson Language Translator](#)” on page 847.

4. Choose an option in **Relationship Type**:
 - Children
 - Parents
 - Descendants
 - Ancestors
 - Siblings
5. Choose an **Object Type** (displays for all relationship types except siblings). The objects that are listed vary depending on what you chose in **Relationship Type**.
6. Choose a **Parent Object Type** and a **Sibling Object Type** (displays only if **Relationship Type** is **Siblings**).
7. Choose an option in **Chart Type**:
 - Bar
 - Doughnut
 - Gantt
 - Heat Map
 - Horizontal Bar
 - Pie
 - Single Stacked Bar
 - Trend
8. If you choose Gantt, complete the Gantt Chart Configuration fields:
 - a) Select a **Start Date Field**.
 - b) Select an **End Date Field**.
 - c) Select a **Primary Row Field**.
 - d) Optional: Select a **Secondary Row Field**.
 - e) Select a **Color Definition Field**.
 - f) Click **Done**.

For more information about Gantt charts, see “[Chart diagram examples](#)” on page 296.
9. If you choose Heat Map, complete the following fields:
 - a) Select a field in **Horizontal Axis Field**.
 - b) Select a field in **Vertical Axis Field**.
 - c) Choose Count-based or Zone-based in **Color Assignment Type**.
 - d) Choose Categorical or Monochromatic in **Color Palette**.

The next field that is displayed is either **Color Ranges** or **Chart Colors**, depending on whether the heat map is count-based or zone-based.

e) Assign colors to count ranges in **Color Ranges** (count-based only). For more information about color ranges, see “[Colors for field value ranges](#)” on page 158.

f) The heat map is pre-displayed in **Chart Colors** (zone-based only). Assign a color to each cell.

Enumerated values that are defined as hidden are not displayed in **Chart Colors**. However, enumerated values that are hidden are displayed as gray when the heat map is rendered if the value has data.

g) Add rules (optional) and click **Done**. Disregard the steps below.

10. Select a **Public Filter**, if one exists for the object type (optional).

11. Choose a **Relationship Paths** (displays only if **Relationship Type** is Ancestors or Descendants).

12. Choose a field in **Chart Data Field** (displays for all types of charts except Gantt and heat map).

13. In **Method Type** choose Count, Sum, Average, Min, or Max (displays for all types of charts except Gantt and heat map). If you chose Sum, Average, Min, or Max, provide a field in **Aggregation Field**. Only currency, decimal, and integer type fields are displayed in **Aggregation Field**.

For more information, see “[Examples: Bar charts](#)” on page 297.

14. Choose Categorical or Monochromatic in **Color Palette** (displays for all types of charts except Gantt).

15. In **Chart Colors**, apply colors to field values (displays for all types of charts except heat map).

For information, see “[Defining enumerated string fields](#)” on page 170.

16. Add rules to the relationship field (optional). For information, see “[Adding rules to relationship fields](#)” on page 311.

17. Click **Done**.

What to do next

Place the chart in a tab group (optional). For more information, see “[Organizing relationship fields in tab groups](#)” on page 312.

Chart diagram examples

Example: Doughnut chart

In the following example, a Business Entity is open and the doughnut chart shows its related risks by residual risk ratings. Click in the chart to drill down to the underlying objects.

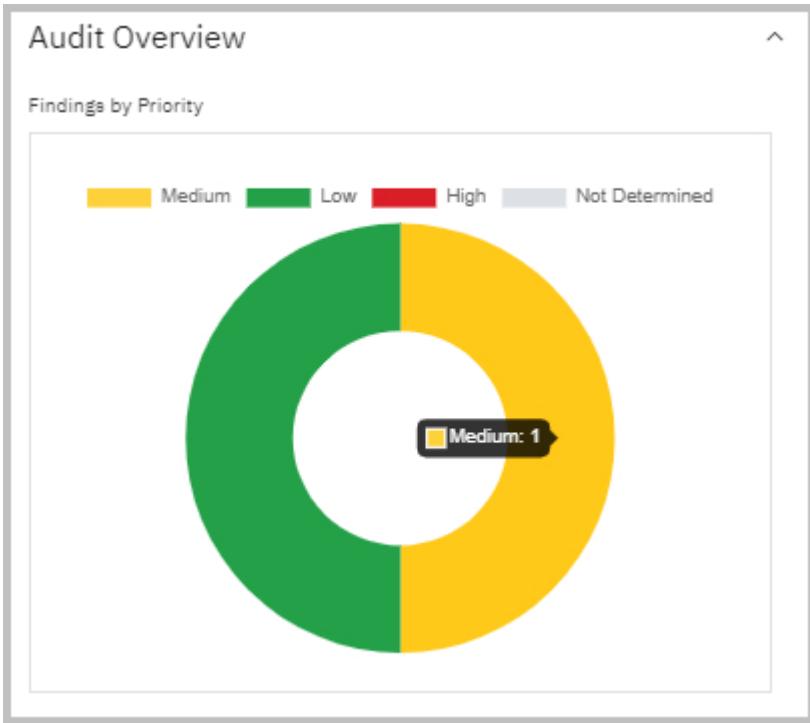


Figure 37. Example of a doughnut chart

Examples: Bar charts

In the following examples, a bar chart on the Dashboard is based on Loss Events. The **Chart Data Field** is set to Risk Category, which defines the colored bars in the chart.

In the following example, the **Method Type** is defined as Count. The results is that the chart shows the number of objects in each Risk Category.

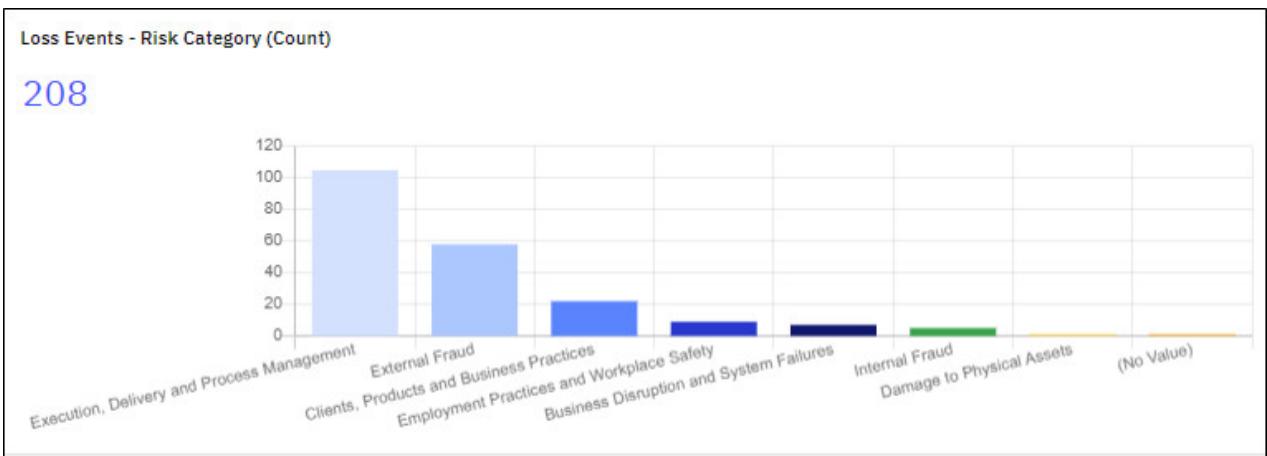


Figure 38. Bar chart with Method Type defined as Count

In the following example, the **Method Type** is defined as Max and the **Aggregation Field** is set to Gross Loss. The result is that the chart shows the maximum Gross Loss value for objects in each Risk Category.

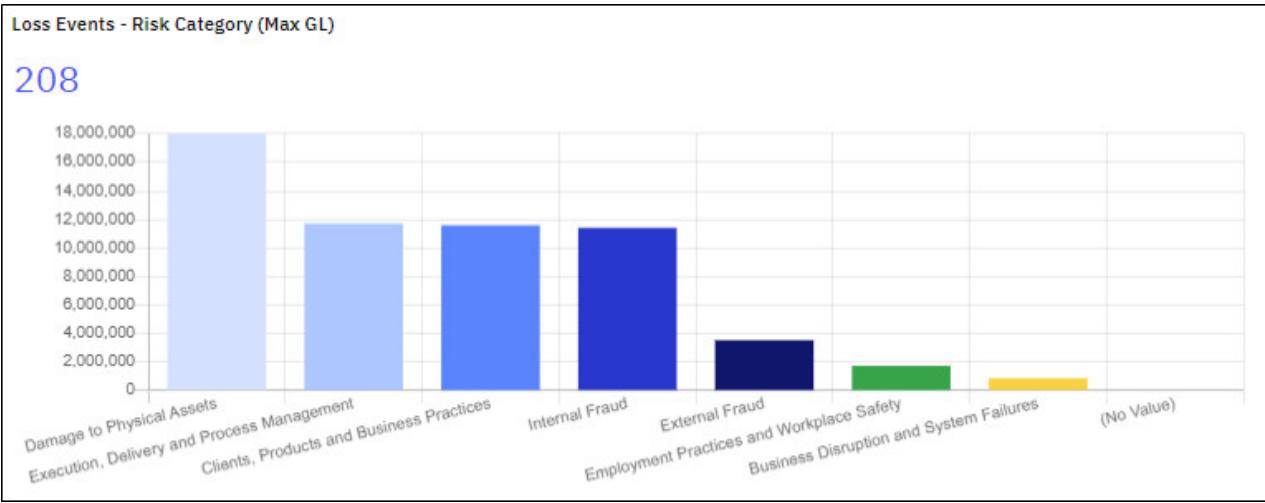


Figure 39. Bar chart with Method Type defined as Max and Aggregation Field set to Gross Loss

Example: Gantt chart

Use a Gantt chart when you want to view project or task assignment status over time. Gantt charts are typically used to view work assigned to a team or an individual person.

When you define a Gantt chart, you define the fields that make up the horizontal and vertical axes:

- The horizontal axis is a date range of two date fields that you choose. Note that system date fields cannot be used as date fields in Gantt charts.
- The vertical axis is one mandatory field and one optional field on the object type.

The order of the dates on the horizontal axis increases from left to right. The order of the fields on the vertical axis depends on the field definition. For string values, the order is alphabetical. For enumerated values, the order is the same as the order that is declared in the field definition if it is an enumerated value. The order of both axes is fixed and cannot be changed.

A Gantt chart can be opened from the following access points:

- A Task View
- A Dashboard panel that a user created
- A Dashboard panel that an administrator created

The access point determines how filtering is applied. If a Gantt chart is opened from:

- A Task View, a public filter can be defined in the Gantt chart.
- A Dashboard panel that a user created, either a public or private filter can be defined in the Dashboard panel.
- A Dashboard panel that an administrator created, a public filter can be defined in the Dashboard panel.

The access point determines what happens when you click a row in a Gantt chart. If a Gantt chart is opened from:

- A Task View, the object opens in a Quick View.
- A Dashboard, the object opens in a Task View in a new tab.

Coloring in a Gantt chart depends on colors assigned to the primary and secondary fields. If no colors are assigned to the field values in a view, the rows display as gray. If the field values are assigned a color in a view, those colors are applied. To override the colors or if neither field is an enumerated field, you must define colors in **Color Definition Field**.

Gantt charts become less useful when they contain a lot of data. For this reason, apply filters and keep the date range short. Up to 425 items can be displayed vertically.

For example, a useful Gantt chart is one that shows Plans that are associated with an Audit. The horizontal axis can show the date range of Expected Start Date to Expected End Date. The vertical axis can list the auditors and activities.

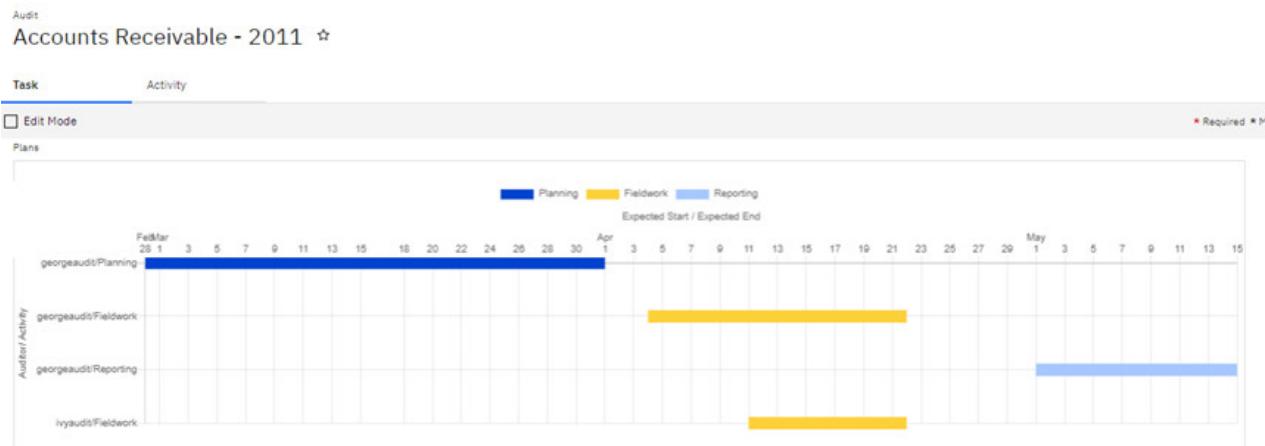


Figure 40. Gantt chart

Example: Heat map (count-based)

Use a count-based heat map when you want to see a data distribution chart, where colors are assigned to counts rather than zones in the chart. You use the colors to apply emphasis to the counts in the chart.

When you define a count-based heat map, you define the two fields that make up the horizontal and vertical axes and the colors for the enumerated value ranges.

The order of the values on the horizontal axis is the same as the order that is declared in the field definition. The same is true for the vertical axis but the order is reversed. The order can be changed in the field definition, but the order of the items in all drop downs is affected.

In the following example, a Business Entity is open and a count-based heat map chart shows its related loss events. Each cell contains a count of objects at value intersect points for Risk Category and Business Line. There are, for example, 32 loss events categorized as External Fraud and Asset Management. A user can click in a cell to drill down to the underlying objects.

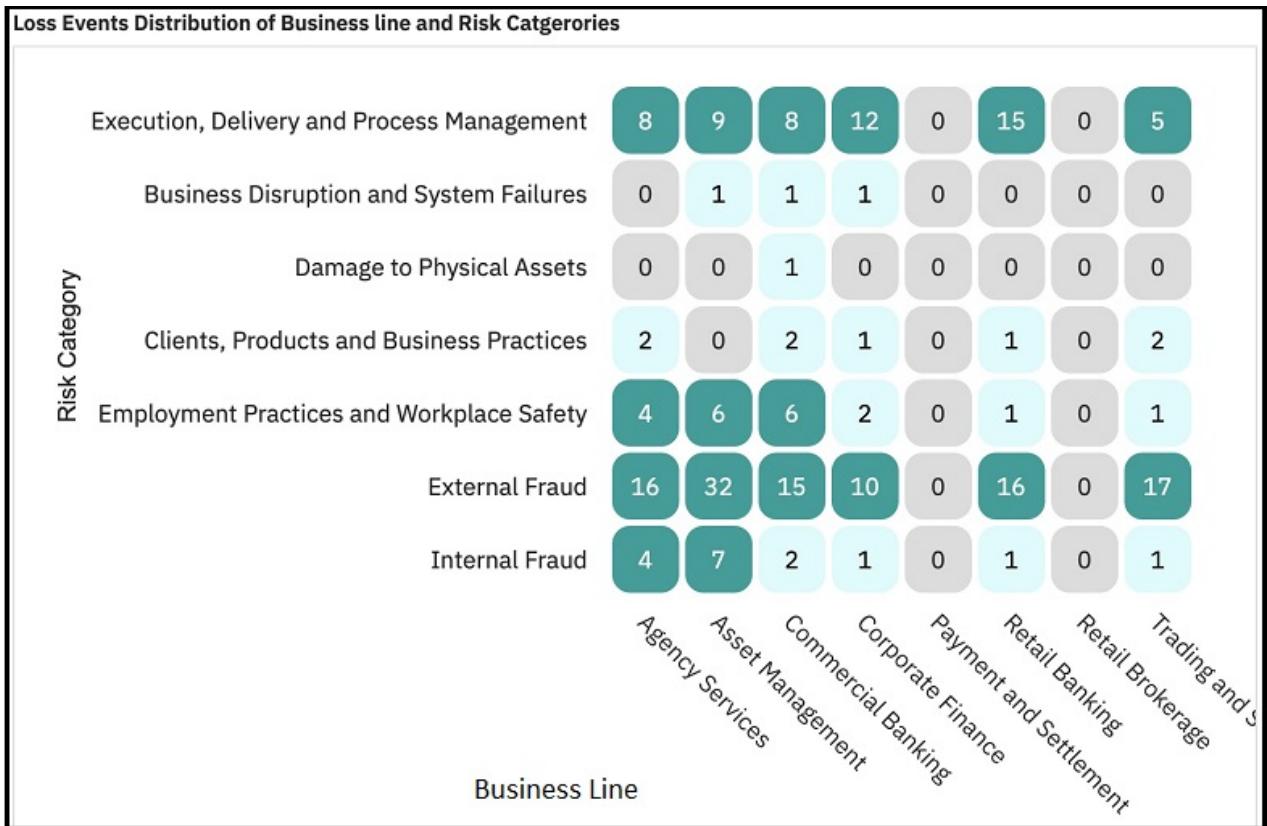


Figure 41. Count-based heat map based on Risk Category (vertical axis) and Business Line (horizontal axis)

Example: Heat map (zone-based)

Use a count-based heat map when you want to see a data distribution chart, where colors are assigned to cells in the chart rather than counts. You use the colors to apply emphasis to the value intersects in the chart.

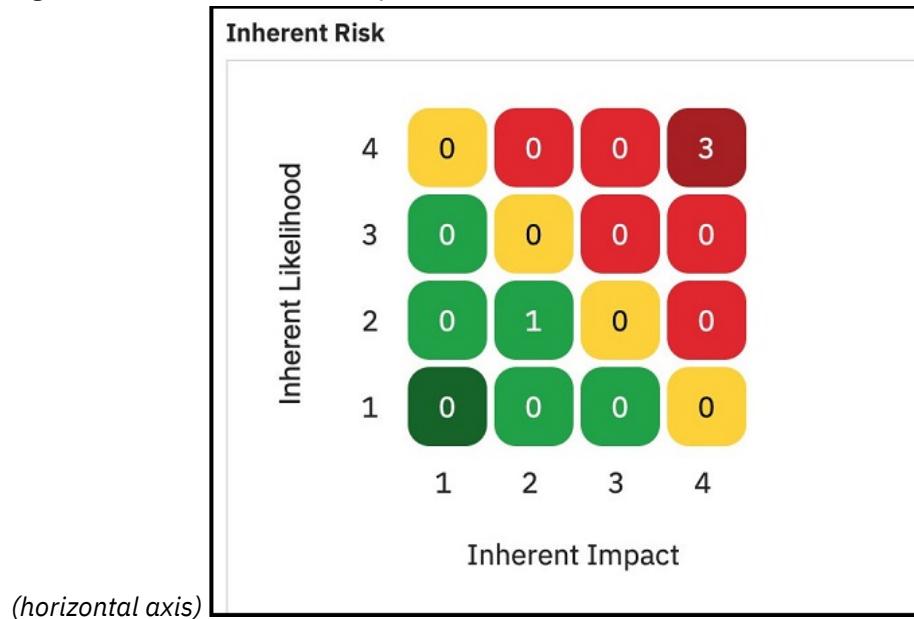
When you define a zone-based heat map, you define the two fields that make up the horizontal and vertical axes, and assign colors to cells (zones) in the map.

The order of the values on the horizontal axis is the same as the order that is declared in the field definition. The same is true for the vertical axis but the order is reversed. The order can be changed in the field definition, but the order of the items in all drop downs is affected.

In the following example, a Risk Assessment is open and a zone-based heat map chart shows its related risks organized by inherent risk. Each cell contains a count of objects that have value intersects for Inherent Likelihood and Inherent Impact. There are, for example, 3 risks whose Inherent Likelihood and Inherent Impact are both 4. Regardless of the count, the value intersect where Inherent Likelihood and Inherent Impact are both 4 is always red and in the upper right corner.

A user can click in a cell to drill down to the underlying objects.

Figure 42. Zone-based heat map based on Inherent Likelihood (vertical axis) and Inherent Impact (horizontal axis)



Example: Horizontal bar

In the following example, an Audit is open and a horizontal bar chart shows its related work papers by review status. Click in the chart to drill down.

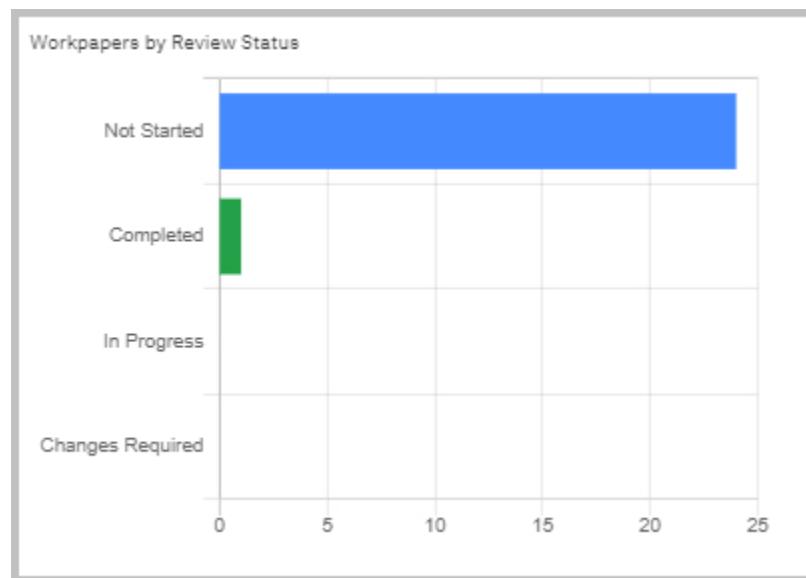


Figure 43. Example of a horizontal bar chart

Example: Single stack bar

In the following example, an Audit Section is open and a single stack bar chart shows its related Workpapers by review status. You can quickly understand that most of the Workpapers for this Audit Section are complete.

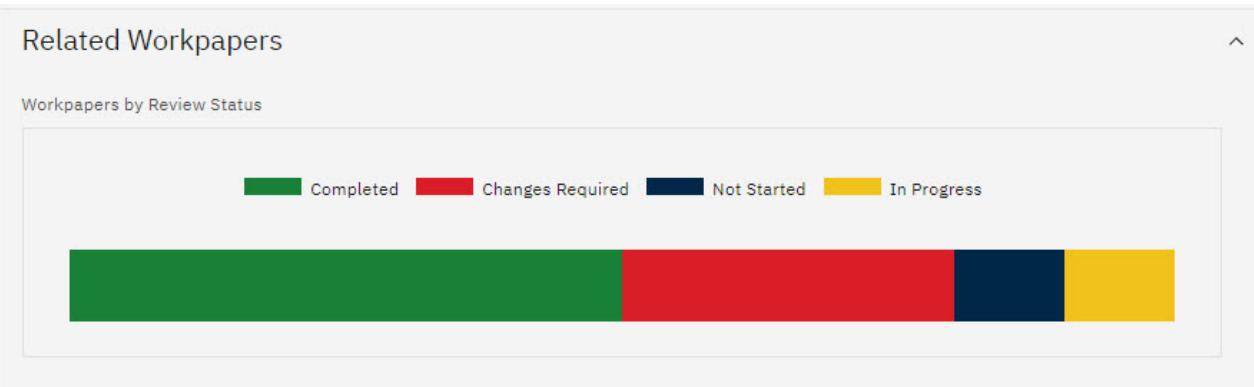


Figure 44. Example of a single stack bar chart

Click in the different areas of a chart to open a Grid View that lists the underlying objects for that value.

For example, click in the **Completed** area and a Grid View opens that lists Workpapers that are related to this Audit Section and whose review status is **Completed**.

Indicators at the top of the Grid View show the filters that are applied and the number of objects in the list. Click the arrow icon to open the parent object. Click **X** to remove a filter and update the list in the Grid View.

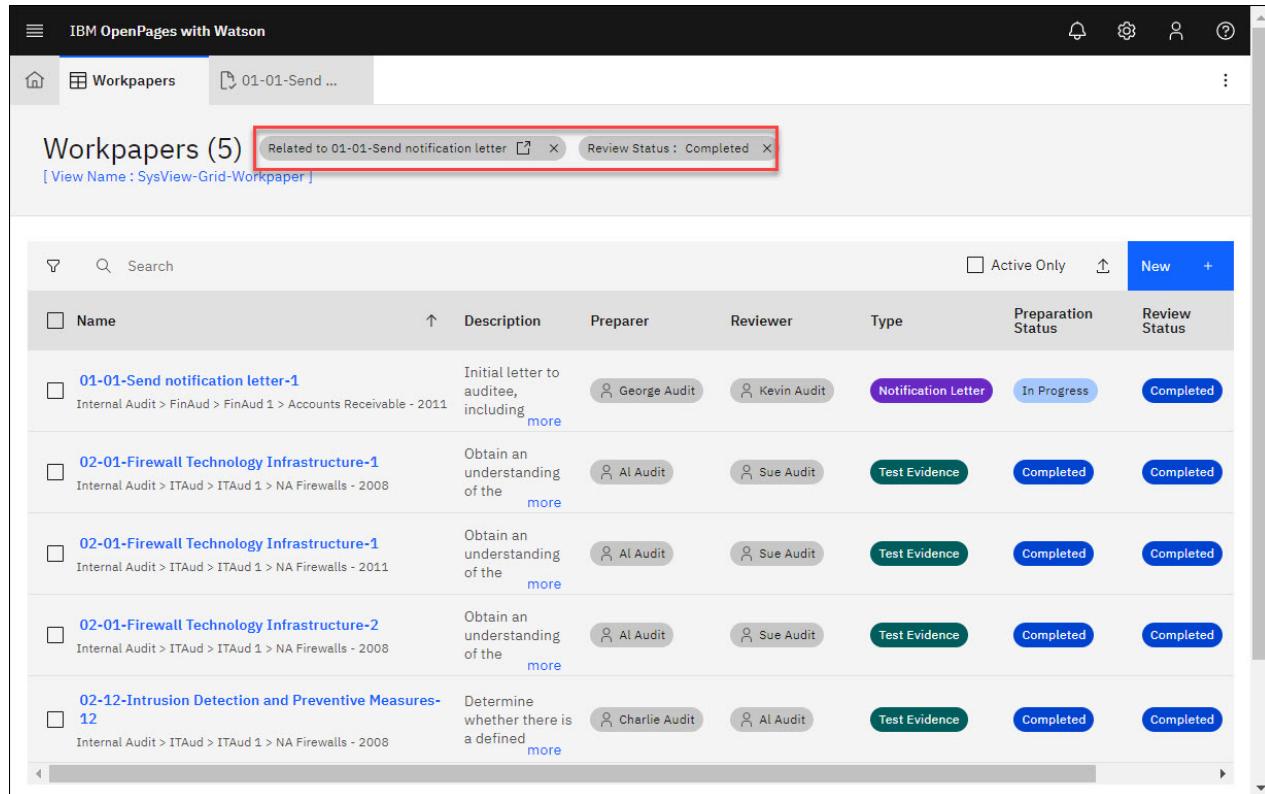


Figure 45. Grid View of underlying objects in a chart

Example: Trend chart

Use a trend chart to display the trends of numeric values of child objects over time. The following example shows a trend chart on the KRI Task View. The chart displays the **Value** field of child KRI Value objects in blue, the **Red Threshold** values, and the **Yellow Threshold** values.

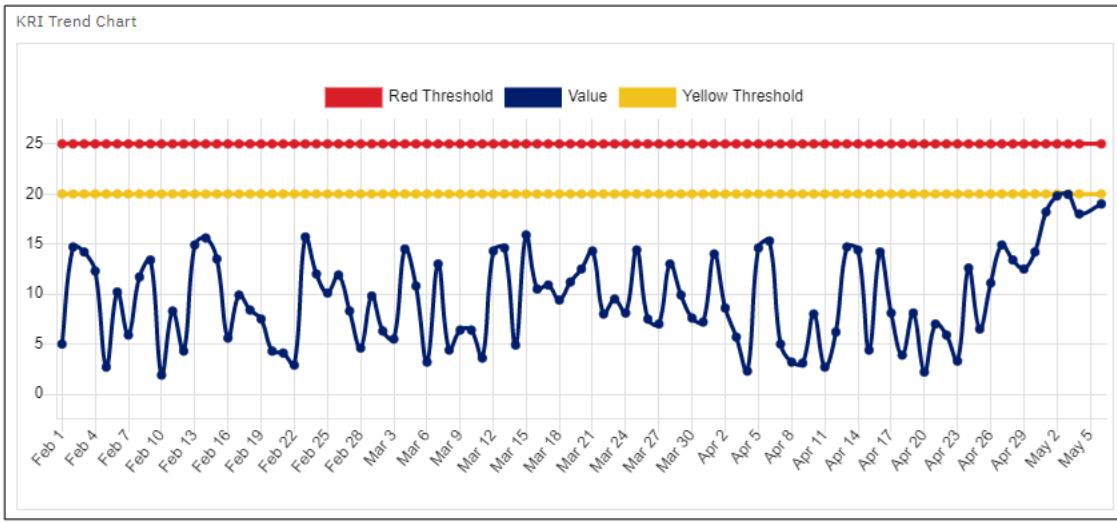


Figure 46. A KRI trend chart

Adding a count

Use a count to provide quick access to items that need to be worked on. Valid in Task Views.

About this task

Counts are valid in Task Views.

A count shows an object count. Click the count to open a Grid View that lists parent or child objects.

The **Relationship Type** property controls the object relationships that are included in the count diagram.

The **Object Type** property controls the object type that is counted.

Color palettes cannot be applied to counts.

In the following example, a risk assessment is open and the count is for SOXControl objects. You can see how many objects exist and drill down into the count.

Controls
40

On the JSON tab, a count is defined with `type` as `relationship` and `subDisplayType` as `count`.

Procedure

1. In the View Designer, click the **Design** tab.
The palette is displayed.
2. Drag a Count element from the palette and add it to a group or a section.
3. Enter a **Label**. It displays as a field header within a section. Click **Edit** to enter localized values.

If it is displayed, click to populate translated values to languages. For more information, see “IBM Watson Language Translator” on page 847.

4. Choose an option in **Relationship Type**:

- Children
- Parents
- Descendants
- Ancestors

- Siblings
- Choose an **Object Type** (displays for all relationship types except siblings). The objects that are listed vary depending on what you chose in **Relationship Type**.
 - Choose a **Parent Object Type** and a **Sibling Object Type** (displays only if **Relationship Type** is Siblings).
 - Select a **Public Filter**, if one exists for the object type (optional).
 - Choose a **Relationship Paths** (displays only if **Relationship Type** is Ancestors or Descendants).
 - Define **Color Ranges**.

For information, see “[Colors for field value ranges](#)” on page 158.
 - Add rules to the relationship field (optional). For information, see “[Adding rules to relationship fields](#)” on page 311.
 - Click **Done**.

Adding a grid layout

Use a grid layout to add parent and child objects, compare objects, upload files (attachments), and select objects to work on.

About this task

Grid layouts are valid in Creation, Task, and Admin Views.

A grid shows related objects in a table and supports actions. It is well suited, for example, for uploading files and adding parent or child objects.

From an Admin or Task View, objects that are listed in a grid are initially sorted alphabetically by object name. The user can then change the sorting. From a Creation View, objects that are listed in a grid are not initially sorted, and the user cannot change the sorting.

From a Task View, if you click a row in the grid, the object opens in a Task View in a new tab.

If you click  next to an object in the grid, the object opens in a Quick View. A Quick View is a Task View that is displayed in a small sidebar. A Quick View has all the functionality of a Task View with a few exceptions. Quick View is always available in a grid layout and requires no configuration.

From a Task View, if you click the field label of the relationship field, a Grid View with the same filter criteria opens. You can move between this Grid View and the Task View where you started.

A search box is always displayed in Task and Admin Views. A search box is not displayed in a Creation View.

Consider performance when you design Grid relationship fields for object types that potentially display a large number of objects. For quicker system performance, apply a public filter to a relationship field. On actions, apply folder filters and filter rules.

The **Fields** property controls the fields that are displayed in the relationship field. You can control what field the information is sorted by and the sort order.

To use the relationship field to upload files in task views, choose File in **Object Type**. The **Fields** property includes only **File Name** by default. You can optionally add other fields to display in the relationship field. If **Description** is not included in the **Fields** property, a user can still add a description when they select a file to upload.

Note: If you edit the JSON and make **Description** read-only, a user cannot add a description when they select a file to upload. If you make **Description** required and read-only, a user cannot upload a file.

Additionally, you must define a task view for files (SOXDocument). For information, see “[Defining Task Views for file object types](#)” on page 269. It is not possible to upload files in a Creation View.

If you choose an actor field in **Sort By**, the values are sorted by username (not first name and last name). The sort is case-sensitive.

In the following example, a new business entity object is open and you can add a primary parent business entity.

The screenshot shows the IBM OpenPages with Watson interface. At the top, there is a navigation bar with icons for Home, Abrucca Limi..., Accounts Re..., Issues, Business Ent..., and a New Business Entity button. The main area is titled "New Business Entity". A modal dialog is open, titled "Select Primary Business Entity". The dialog lists 336 total entities. It has three search fields: "Search", "Search in folder", and "Search users". The results table has columns for "Name" and "Description". The first result is "Abrucca Limited" (Legal Entity). Other results include "Africa and Middle East" (Africa and Middle East), "Agency Services" (Organisational Unit), "Agency Services" (Organisational Unit), "Agency Services" (Organisational Unit), and "Asia". At the bottom of the modal, there are "Cancel" and "Done" buttons. The "Done" button is highlighted with a blue background.

Figure 47. Example 1: Adding a primary parent

In the following example, an admin view contains **Parents** and **Children** grid relationships. A Control object is open. In the **Parents** grid, you can add a parent by clicking **Add** or set a primary parent by clicking **Set primary parent**. In the **Children** grid, you can add a child by clicking **Add** or create a new child by clicking **New**.

Figure 48. Example 2: Parents and children of a Control object

You can find grid view examples in SysView-Task-SOXBusEntity and SysView-Task-SOXControl.

On the JSON tab, a grid layout is defined with `type` as `relationship` and `subDisplayType` as `grid`.

Procedure

1. In the View Designer, click the **Design** tab.
The palette is displayed.
2. Drag a Grid element from the palette and add it to a section.
3. Enter a **Label**. It displays as a field header within a section. Click **Edit** to enter localized values.

If it is displayed, click **Auto Translate** to populate translated values to languages. For more information, see “IBM Watson Language Translator” on page 847.

4. Choose an option in **Relationship Type**:
 - Children
 - Parents
 - Descendants
 - Ancestors
 - Siblings
5. Choose an **Object Type** (displays for all relationship types except siblings). The objects that are listed vary depending on what you chose in **Relationship Type**.
6. Choose a **Parent Object Type** and a **Sibling Object Type** (displays only if **Relationship Type** is Siblings).

7. Select a **Public Filter**, if one exists for the object type (optional).
8. Click **Add Action** to display an action button in the card (displays only if **Relationship Type** is Children or Parents).

If **Relationship Type** is Children, you can add the following types of actions:

- Add
- Copy Recursive
- Delete
- New
- Watson Suggestions

If **Relationship Type** is Parents, you can add the following types of actions:

- Add
- Set Primary Parent
- Watson Suggestions

For information about actions, see [“Adding actions to relationship fields” on page 313](#).

9. Choose a **Relationship Paths** (displays only if **Relationship Type** is Ancestors or Descendants).
10. Set **Required** to true to make it mandatory for a user to provide at least one object in the grid.
11. Choose a field in **Sort By**.
12. Define the **Sort Direction**.
13. Add rules to the relationship field (optional). For information, see [“Adding rules to relationship fields” on page 311](#).
14. Click **Done**.

What to do next

Place the grid in a tab group (optional). For more information, see [“Organizing relationship fields in tab groups” on page 312](#).

Adding a tree diagram

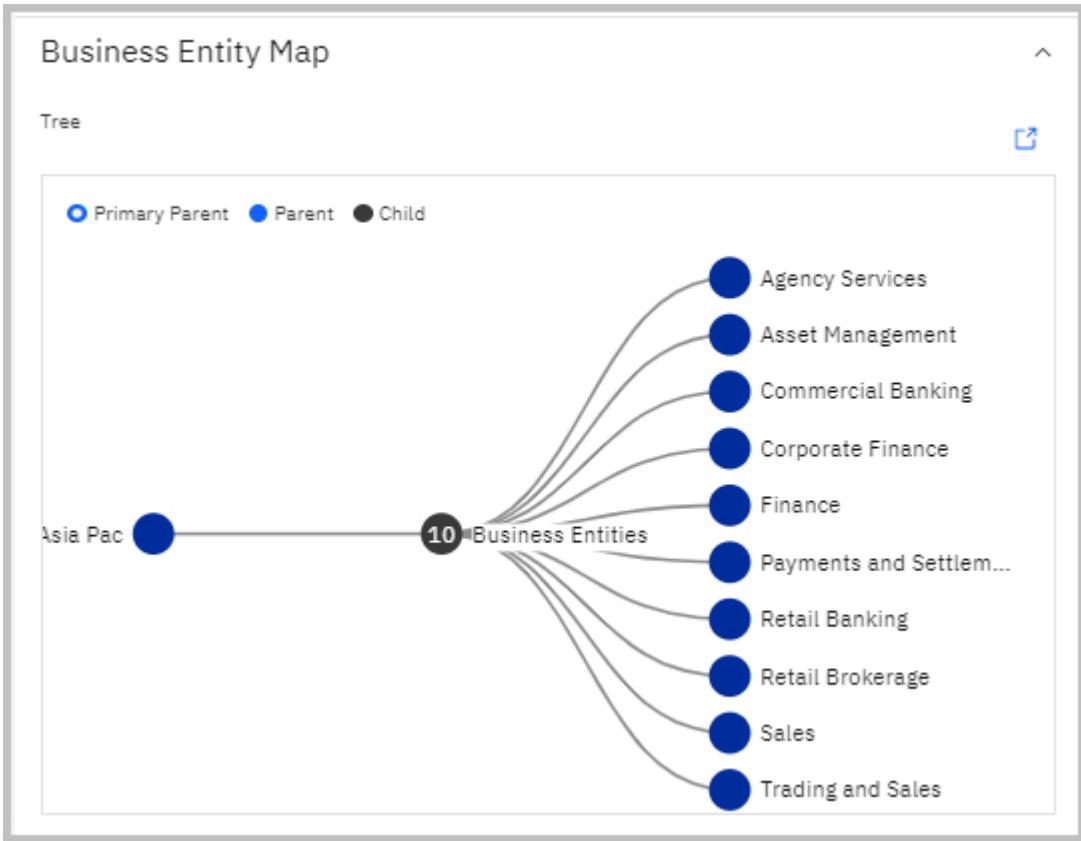
Use a tree diagram to display an object relationship diagram that allows users to interactively explore data and data relationships.

About this task

Tree diagrams are valid in Task Views.

A tree diagram displays an object relationship structure. You can see how an object is related to all other objects, parent objects, or child objects. You can also drill through the diagram and open objects.

In the following example, a business entity is open and all parent and child objects are displayed in a tree diagram.



You can find an example in: [SysView-Task-SOXBusEntity](#).

On the JSON tab, a tree diagram is defined with `type` as `relationship` and `subDisplayType` as `tree`.

Procedure

1. In the View Designer, click the **Design** tab.
The palette is displayed.
2. Drag a Tree element from the palette and add it to a section.
3. Choose an option in **Relationship Type**:
 - blank (includes both Children and Parents)
 - Children
 - Parents
4. Add rules to the relationship field (optional). For information, see [“Adding rules to relationship fields” on page 311](#).
5. Click **Done**.

What to do next

Place the card in a tab group (optional). For more information, see [“Organizing relationship fields in tab groups” on page 312](#).

Adding a classifier field that makes object association suggestions

You can add classifier fields that make object association suggestions using a natural language processing service.

Before you begin

The natural language processing service must already be configured to make object association suggestions. For information, see [“Natural language processing services ” on page 850](#).

About this task

Classifier fields that make object association suggestions are valid in Creation Views and Task Views.

The UI supports making taxonomy suggestions and object association suggestions. For information about taxonomy suggestions, see [“Adding a classifier field that makes taxonomy suggestions ” on page 288](#).

You can add multiple classifier fields to a view.

The classifier field and the classifier input field must both be in the view. The classifier target fields can optionally be included in the view. It is not necessary to configure the Watson statement on the classifier input field (*Adding a description improves IBM Watson Suggestions*), the IBM Watson Insights button, or the IBM Watson Insights panel. These elements display automatically for classifier fields.

The action label is the button label for the IBM Watson Insights button. The title of the IBM Watson Insights panel is the object type plus *Mapping*.

In this example, the text in the Description on a new Issue is used as input to a natural language processing service that can suggest appropriate Controls. The field that associates Controls is configured to be a classifier field.

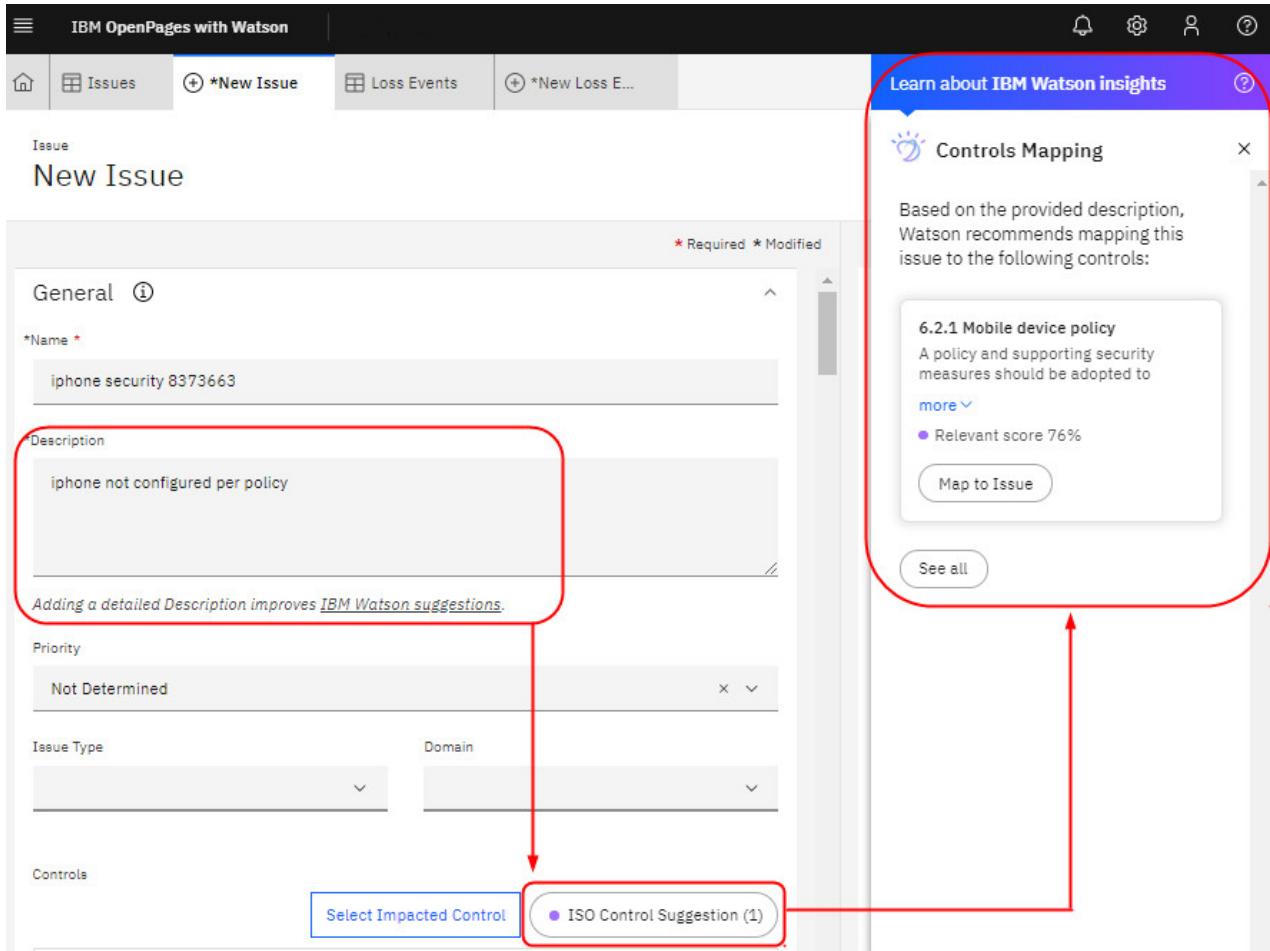


Figure 49. Example of a Classifier field that makes taxonomy suggestions

On the JSON tab, a classifier field is part of a card or grid relationship field and its `actionType` is set to `suggestAssociations`.

Procedure

1. Drag the classifier input field either from the palette or the canvas and add it to a section or group.
2. Drag the classifier field either from the palette or the canvas and add it to a section or group.
3. Create a card or grid relationship field and follow all steps until you define an action. For information, see [“Adding a card layout” on page 292](#) or [“Adding a grid layout” on page 304](#).
4. Click **Add Action** and choose **Watson Suggestion**.
 - a) Enter a **Label**. It displays as a button label. Click **Edit** to enter localized values.

If it is displayed, click **Auto Translate** to populate translated values to languages. For more information, see [“IBM Watson Language Translator” on page 847](#).
 - b) Select the classifier field you already put on the canvas in **Classifier Field**. The system lists only classifier fields that are on the canvas.

Although it is not required, it might make sense to place the classifier field near the card or grid relationship field that uses it.
 - c) Click **Done**.
5. Finish defining the relationship field.

Adding rules to relationship fields

You can apply **Rules** to all types of relationship fields (cards, charts, counts, grids, and trees).

About this task

Rules allow you to more precisely control whether a relationship field is visible or hidden. For cards and grids, rules can also control some aspects of what users can do with related objects.

Rules on relationship fields are based on the fields for the object type of the view. For example, if you are building a view for Risk objects and the relationship field is for Control objects, the rules are based on fields for the Risk object not the Control object.

In a rule, you specify a condition that checks for the existence of any value of a field or specific values of one or more fields on an object. If the condition is met, the rule is applied to the relationship field.

In all types of relationship fields (cards, charts, counts, grids, and trees), you can apply the following rule types:

- **Visible**
Shows the relationship field in a view if the rule is met.
- **Hidden**
Hides the relationship field in a view if the rule is met.

In cards and grids, you can apply the following additional rule types:

- **Editable**
Makes buttons in a card or grid visible and actionable if the rule is met.
- **Read Only**
Hides buttons in a card or grid if the rule is met. Users can view objects in the card or grid but cannot change them.
- **Required**
Makes it mandatory for the user to provide one object in a card or grid if the rule is met.

Procedure

1. In the View Designer, click the **Design** tab.
The palette is displayed.
2. First, move the fields that are used in the rule from the palette to the canvas.
In the following steps, the options in **Rule Type** vary depending on the relationship field type.
3. In the property panel of a relationship field, click **New Rule**.
4. Select a **Rule Type**.
5. In **Controlled By**, choose **One field with any value** or **Multiple controllers or values**.
6. If you choose **One field with any value**:
 - a) Select a **Controlling Field**. The system lists fields for the object type of the view that are on the canvas.
 - b) Click **Done**.
7. If you choose **Multiple controllers or values**:
 - a) In **Controlling Field Logic** select **All controlling field conditions must be met** or **Any controlling field condition may be met**.
 - b) Click **New Controller**.
 - c) Choose a field in **Controlling Field**. The system lists fields for the object type of the view that are on the canvas. The next selections depend on the field type.

- For actor fields, you can set **Match Current User** and/or select other users or user groups in **Other Users or Groups**. Any match on either field resolves the controller to true. If **Match Current User** is set to true, the signed on user must be the user or be in a user group for the value in the **Controlling Field**.
 - For enumerated type fields, click **Values** and you can choose one or more individual values.
 - Click **Done**.
- d) Click **New Controller** to add the next controller field. Repeat the previous steps. Continue until all controller fields have been added. Although you can change the order of the controller fields, it has no effect in the view.

8. Click **Done**.

Organizing relationship fields in tab groups

You can organize the following types of relationship fields in tab groups: cards, charts, grids, and trees. Counts cannot be placed in tab groups.

About this task

Use tab groups to maximize the use of space and improve usability. Without tabs, relationship fields are listed vertically down the page and users must scroll down to view them.

A tab group can have up to six relationship fields. Each relationship field displays as a tab. The name of the relationship field is the tab label.

Tab groups can be added to Creation Views and Task Views. A Creation View or Task View can have multiple tab groups.

In the following example, a Risk object is open and six relationship fields are displayed in a tab group named, Tab Group Section. The first tab, Mitigating Controls, is open, and it is a grid relationship field.

Name	Control Owner	Design Effectiveness	Operating Effectiveness
CTL-04-03-03-01 Global Financial Services > North America > Retail Banking	fcm	Effective	Not Determined
CTL-04-03-03-02 Global Financial Services > North America > Retail Banking	orm	Effective	Not Determined
CTL-04-03-03-03 Global Financial Services > North America > Retail Banking	iam	Not Determined	Not Determined

Procedure

1. In the View Designer, click the **Design** tab.
The palette is displayed.
2. Drag a Tab Group from the palette to the canvas and place it in a section.
3. Enter a **Name**.
4. Click **Done**.
5. Add relationship fields to the tab group. Either create a new relationship field or drag an existing one from the canvas to the tab group.
6. Move the relationship fields up and down to control the order from left to right that they are displayed in the tab group.

Adding actions to relationship fields

You can use actions on relationship fields to create, copy, delete, associate, or disassociate objects.

You can add one or multiple actions to card and grid relationship fields.

Adding an Add action

Define an action as **Add** to associate parent or child objects. When a user clicks **Add**, a Grid View opens where the user can select objects.

About this task

Use an **Add** action, for example, on a Task View for loss events if you want to add the ability to associate mandates.

A grid or card relationship field that is defined with an **Add** action displays a **Remove** button when one or more associated objects are selected. The **Remove** button allows you to disassociate objects (it does not delete objects). If the relationship field is required, all associated objects can be removed except for one. The **Remove** button displays automatically when an **Add** action is configured for a relationship field.

To delete objects, use the **Delete** action. A **Delete** button is displayed when one or more associated objects are selected. For information about providing the ability to delete objects, see [“Adding a Delete action” on page 317](#).

To associate a primary parent object, use the **Set Primary Parent** action rather than **Add**. For information, see [“Adding a Set Primary Parent action” on page 314](#).

You can find an example in: SysView-Task-LossEvent.

On the JSON tab, an associate action is defined when *actionType* is set to associate in a card or grid relationship field.

Procedure

1. In a card or grid relationship field, click **Add Action** and choose **Add**.
2. Enter a **Label**. It displays as a button label. Click **Edit** to enter localized values.

If it is displayed, click  to populate translated values to languages. For more information, see [“IBM Watson Language Translator” on page 847](#).

3. Set **Multi Select** to true or false.
4. Click **Folder Filter** to restrict the objects that are available for selection in the Grid View to a specific folder.
5. Click **Filter Rules** to restrict the objects that are available for selection in the Grid View using a dynamic filter. For information see, [“Defining dynamic filters on actions in relationship fields” on page 317](#).

6. Click **Done**.

Results

If both **Folder Filter** and **Filter Rules** are provided, the filters are combined with an AND statement. An object must match both filters to be available for selection.

Adding a Set Primary Parent action

Define an action as **Set Primary Parent** to associate a parent object or to change the current primary parent. When a user clicks **Set Primary Parent**, a Grid View opens where the user can select an object as the primary parent. If the object does not have a primary parent, the parent object chosen by the user is set to the primary parent. If the object has a primary parent, the parent object chosen by the user overrides it as the primary parent, but remains as a parent.

About this task

For most object types, a Creation View must have a relationship field with a **Set Primary Parent** action or an **Add** action.

For example, you can add the following actions to a Task View for loss events if you want to add the ability to add a primary parent and other business entities:

- A **Set Primary Parent** action.
- An **Add** action. When a user adds the first object, that object is automatically set as the primary parent.

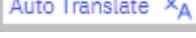
A **Set Primary Parent** action does not display a **Remove** button when one or more already associated objects are selected. To display a **Remove** button, add an **Add** action to the relationship field. The primary parent itself cannot be removed, but other objects can be. To remove a primary parent, choose another object as the primary parent, and use **Remove** to disassociate the former primary parent. For more information, see “[Adding an Add action](#)” on page 313.

You can find an example in: SysView-Task-LossEvent.

On the JSON tab, an associate primary parent action is defined when *actionType* is set to *associatePrimary* in a card or grid relationship field.

Procedure

1. In a card or grid relationship field, click **Add Action** and choose **Set Primary Parent**.
2. Enter a **Label**. It displays as a button label. Click **Edit** to enter localized values.

If it is displayed, click  to populate translated values to languages. For more information, see “[IBM Watson Language Translator](#)” on page 847.

3. Click **Folder Filter** to restrict the objects that are available for selection in the Grid View to a specific folder.
4. Click **Filter Rules** to restrict the objects that are available for selection in the Grid View using a dynamic filter. For information see, “[Defining dynamic filters on actions in relationship fields](#)” on page 317.
5. Click **Done**.

Results

If both **Folder Filter** and **Filter Rules** are provided, the filters are combined with an AND statement. An object must match both filters to be available for selection.

Adding a New action

Define an action as **New** to create a new object. The Creation View for the object type opens. The New action is available only if **Relationship Type** is Children.

About this task

You can find an example in: SysView-Task-LossEvent.

On the JSON tab, a New action is defined when *actionType* is set to addNew in a card or grid relationship field.

Procedure

1. In a grid or card relationship field, click **Add Action** and choose **New**.
2. Enter a **Label**. It displays as a button label. Click **Edit** to enter localized values.

If it is displayed, click  to populate translated values to languages. For more information, see “IBM Watson Language Translator” on page 847.

3. In **New Object Behavior**, choose **Tab** or **Sidebar** to define where the Creation View opens. **Tab** opens the Creation View in a new tab. **Sidebar** opens the Creation View in a Quick View side panel of the Task View that is already open.

If you select **Sidebar**, the Creation View can only create new child objects for the parent object that is open. No other associations are supported in the sidebar. Verify that the Creation View does not contain any other association actions.

4. Click **Done**.

Adding a Copy Recursive action

Define an action as **Copy Recursive** to copy an existing object and associate it to an object that is open in a Task View. The action can be defined to make copies of objects that are associated to a source object and to copy parent associations from a source object to a new object.

About this task

The **Copy Recursive** action can be used in cards and grids in Task Views. The **Relationship Type** must be Children.

A **Copy Recursive** action can be used, for example, in a Task View for Process objects to allow users to make copies of existing Risk and Control objects. When a user accesses the Task View, a grid relationship field displays Risk objects that are already associated with the open Process object and that match a **Public Filter**, if one is defined. When a user clicks a button for the copy action, Risks that meet the **Folder Filter** and **Filter Rules** criteria are listed. The list includes Risks that are already associated with the Process and those that are not. When a user selects a Risk and clicks Done, a copy of the selected source Risk object is created and associated to the Process that is open in the view.

Additionally, depending on how the **Copy Recursive** action is defined, copies are also made of the source object's child and grandchild objects, for a specified object type relationship. Only child objects that have the source object as their primary parent are copied. For example, when a Risk object is copied, copies of all child Control objects that have the Risk as their primary parent can also be made.

Additionally, depending on how the **Copy Recursive** action is defined, parent associations for a source object can be replicated to newly copied objects. For example, a newly copied Control can be associated to the same parent Requirement objects as the source Control object.

Depending on how workflows are configured, workflows can be started for the newly created objects and child objects. Workflows cannot be started on newly created grandchild objects.

On the JSON tab, a copy recursive action is defined when *actionType* is defined as *copyRecursive* in a card or grid relationship field.

Procedure

1. In a card or grid relationship field, click **Add Action** and choose **Copy Recursive**.
2. Enter a **Label**. It displays as a button label. Click **Edit** to enter localized values.

If it is displayed, click **Auto Translate** to populate translated values to languages. For more information, see “IBM Watson Language Translator” on page 847.

3. Click **Folder Filter** to restrict the objects that are available for selection in the Grid View to a specific folder.
4. Click **Filter Rules** to restrict the objects that are available for selection in the Grid View using a dynamic filter. For information see, “Defining dynamic filters on actions in relationship fields” on page 317.
5. Set **Auto Name Children** to true or false. If set to true, auto naming is applied to all newly copied objects (including children and grandchildren) in the object type relationship, given that auto naming is defined for the object type. For information about configuring auto naming, see “Object auto-naming settings” on page 483.
6. For object types that are not configured to use auto naming, the **Conflict Behavior** setting determines what happens when a copied object has the same name as an existing object in a target location. Options are:
 - **Overwrite** - a new version of the object in the target directory is created with all of the information of the copied object. All prior versions of the object in the target directory are maintained.
 - **Copy Of** - during the copy operation, any objects with the same name as an existing object in the target location will be renamed to "Copy of <object name>".

Note: Consider carefully whether to use **Overwrite** or **Copy Of** when you copy objects that have the same name coming from different hierarchies. The end result if you use **Overwrite** will be a single object with many versions. However, if you use **Copy Of**, it will be many objects with one version.

- **Existing** - if a copied object has the same name as an object in the target location, that file will not be copied. All other objects (without duplicate names) will still be copied to the target location.

If you choose this option, you should examine the results of copy operations to determine whether any associations between objects have changed as a result of the copy. For example, if an associated risk is not copied to the new location because an existing risk has the same name, the copied parent process of the risk will be associated with the preexisting risk in the target location.

- **Exception** - a message is displayed and the copy action is not completed.

7. Click **Set in Object Type**. The object type relationship structure from the source object type through its child and grandchild object types is displayed. Select each object type that is included in the recursive copy action.
8. Click **Add Associations** to define whether parent associations of source objects are replicated to newly copied objects.
 - a) Choose a **Child Type**. You can choose the object type for the relationship field or any of the objects types you selected in **Object Type**.
 - b) Choose a **Parent Type**. You can choose only from parent object types for the **Child Type** object type that you selected.

You can define multiple parent associations to replicate to newly created objects.

9. Click **Done**.

Results

If both **Folder Filter** and **Filter Rules** are provided, the filters are combined with an AND statement. An object must match both filters to be available for selection.

Adding a Delete action

Define an action as **Delete** to delete child objects that are associated with an object that is open in a Task View.

About this task

The delete action is available only in grid relationship fields. The **Relationship Type** must be Children.

The delete action deletes selected objects. It is not used to disassociate objects. Use an associate action to provide a means of disassociating child objects from an object that is open in a Task View.

The user must have access permissions that allow them to delete objects.

Procedure

1. In a grid relationship field, click **Add Action** and choose **Delete**.
2. Enter a **Label**. It displays as a button label. Click **Edit** to enter localized values.

If it is displayed, click  to populate translated values to languages. For more information, see “[IBM Watson Language Translator](#)” on page 847.

3. Click **Done**.

Adding a Get Watson Suggestion action

Define an action as **Get Watson Suggestion** to specify a field to make object association suggestions.

About this task

For more information, see “[Adding a classifier field that makes object association suggestions](#)” on page 309.

Defining dynamic filters on actions in relationship fields

You can use **Filter Rules** to add dynamic filters to actions in grid and card relationship fields.

About this task

You can use a dynamic filter on an action when you want to reduce the number of related objects that a user can choose from and ensure that the list is appropriate for the object that is open. For example, in a Task View for Risk objects, when a user clicks **Select Controls** and a Grid View opens, you might want to show a list of related controls that are in the same risk category as the Risk object that is open.

The filter is dynamic in the sense that the related objects that are listed in a Grid View are determined when the view is actually used.

Dynamic filters work only:

- For the **Associate**, **Associate Primary Parent**, or **Copy Recursive** actions.
- For direct (parent and child) relationships.

When you define a **Filter Rule**, you set up a field pair. The field pair consists of a field on a related object and a field on the object for the view. The system compares the values in the two fields to determine whether there is a match for the filter. The two fields can either both be text fields or both be enumerated

fields. If the two fields are enumerated fields, they can both be single value, both be multivalued, or be mixed. You can define multiple filter rules. All filter rules are combined with an AND statement.

Dynamic filters do not support the comparison of empty values. If an object has an empty value for the field that is defined in the **Filter Rule**, the rule is ignored.

For more information about rules, see [“Configuring rules” on page 318](#).

On the JSON tab, filter rules are defined in a *filterRules* element in an actions section if *actionType* is *associate*, *associatePrimary*, or *copyRecursive*.

Procedure

1. In a card or grid relationship field, click **Add Action** and choose **Associate**, **Associate Primary Parent**, or **Copy Recursive**.
2. In **Filter Rules**, click **Add Rule**. Establish the field pair that the rule is based on.
 - a) Choose a field in **[object type] field value**. You can choose only from fields on the related object type that is specified in the relationship field. For example, if you are defining a Task View for a Risk object and building a relationship field for a SOXControl object, this field displays as **Control field value**. You can choose only from fields on a SOXControl object.
 - b) Leave **Equals** as is. It cannot be changed.
 - c) Choose a value in **[object type] field value**. You can choose only from fields on the object type for the view and only matching field types for the first field in the field pair. For example, if you are defining a Task View for a Risk object and building a relationship field for a SOXControl object, this field displays as **Risk field value**. You can choose only from fields on a Risk object and only field types that match the field type of the field given in **Control field value**.
 - d) Click **Done**.
 - e) Add more filter rules (optional).
3. Click **Done**.

Configuring rules

The UI includes a framework of rules for field dependencies and validation. Rules ensure that the data that users enter in the UI is valid.

A rule can either provide additional validation of a field's value or alter the behavior of a field, such as hiding a field. Some rules allow you to compare the value of a field with another field, while others compare it to values defined in the rule itself. However, you can't use rules to change or override field dependencies.

Rules are available in Creation, Task, and Admin Views but not in Grid Views. In Task Views, you cannot add rules to fields in the Task View header. Controller fields used in rules must be in the view.

To define rules, go to the **Design** tab in the View Designer. Select a field and click **New Rule** in a field's property panel. Select a **Rule Type** and add conditions. The field type determines what rule types are available. A field can have multiple rule types.

To remove a rule, hover over the rule on the property panel. Click remove and then **Done**.

There are also **Required**, **Editable**, and **Read Only** rule types. These rule types are defined when you click **New Rule**. Use them to define whether a field is required, editable, or read only based on the value of another field in the view, called a *controller* field.

- If **Required** is displayed as a toggle, you can set it to True. In which case, the **Required** rule type is disabled. If you set it to False, you can define a **Required** rule type that determines whether the field is required.
- If **Read Only** is displayed as a toggle, you can set it to True. In which case, the **Editable** and **Read Only** rule types are disabled. If you set it to False, you can define **Editable** or **Read Only** rule types that determine whether the field is read only or editable.

Note: Dependent picklists are not defined in Task or Creation views. However, the views enforce the dependent pick lists that are defined on object types. For more information, see “[Adding and working with dependent picklists](#)” on page 214.

Table 111. Rule Types		
Design	JSON	Description
Editable Read Only	<i>editable</i> <i>readOnly</i>	Makes a field editable or read-only based on the value of one or more other fields.
Visible Hidden	<i>visible</i> <i>hidden</i>	Makes a field visible or hidden based on the value of one or more other fields.
Required	<i>required</i>	Makes a field required based on the value of one or more other fields. In a view, the Save button is disabled until the field is given a value.
Greater than Greater than or equal Less than Less than or equal Equal	<i>greater</i> <i>greaterEqual</i> <i>less</i> <i>lessEqual</i> <i>equal</i>	Validates that a field’s value is greater than, less than, or equal to the value of another field of the same type, or to a value provided in the rule definition. You can define these rules on integer, decimal, date, or currency fields. In a view, a red star is displayed next to the field and the Save button is disabled until the validation passes. The rules can also validate that two text fields have the same value.
Minimum Length Maximum Length	<i>minLength</i> <i>maxLength</i>	Validates that the value of a text field has a minimum or maximum number of characters. In a view, the Save button is disabled until the validation passes. You can define these rules on string fields.
Pattern	<i>pattern</i>	Validates that the value of a text field has a specified format, for example, nnn - nn - nnnn. In a view, the Save button is disabled until the validation passes. You can define this rules on string fields.

Defining Editable and Read Only rules

The **Editable** and **Read Only** rule types make a field editable or read-only depending on the value or values of one or more controller fields in a view.

About this task

You can define **Editable** and **Read Only** rules on any field type.

When you open the property panel for a field, the field type and field definition determine whether the **Required** property is displayed.

The controller fields must be either enumeration or actor fields.

When a field is made read-only because of a change to a controller field, changes to that field’s value since it was last saved are reverted to its original value.

Note: An exception exists for changes to values in grid and card relationship fields. The values cannot be reverted because they are saved immediately.

On the JSON tab, editable and read only rules are defined when *type* is set to `editable` or `readOnly`. Must also specify either a *controllers* or *controllerName* attribute. Specify one or more *controllers* as an array. Use the short-hand format *controllerName* rather than *controllers* to specify only a single *controller* for which ANY value will satisfy the rule's criterion.

In the steps below, select **Editable** or **Read Only** in **Rule Type**.

Procedure

1. In the View Designer, click the **Design** tab.
The palette is displayed.
2. Select the field that you want to add a rule to.
3. In the property panel, click **New Rule**.
4. Select a **Rule Type**.
5. In **Controlled By**, choose **One field with any value** or **Multiple controllers or values**.
6. If you choose **One field with any value**:
 - a) Select a **Controlling Field**.
 - b) Click **Done**.
7. If you choose **Multiple controllers or values**:
 - a) In **Controlling Field Logic** select **All controlling field conditions must be met** or **Any controlling field condition may be met**.
 - b) Click **New Controller**.
 - c) Choose a field in **Controlling Field**. All available controlling fields are displayed. The next selections depend on the field type.
 - For actor fields, you can set **Match Current User** and/or select other users or user groups in **Other Users or Groups**. Any match on either field resolves the controller to true. If **Match Current User** is set to true, the signed on user must be the user or be in a user group for the value in the **Controlling Field**.
 - For enumerated type fields, click **Values** and you can choose one or more individual values.
 - Click **Done**.
 - d) Click **New Controller** to add the next controller field. Repeat the previous steps until all controller fields are added. Although you can change the order of the controller fields, it has no effect in the view.
8. Click **Done**.

Defining Visible and Hidden rules

The **Visible** and **Hidden** rule types make a field or inline guidance for sections either visible or hidden depending on the value or values of one or more controller fields in a view.

Before you begin

About this task

The **Visible** and **Hidden** rule can be defined on any field type and on inline guidance for sections. If a visible field dependency is already defined on a field, you cannot define additional rules of these types on that field in a Task or Creation View.

The *controllers* must be either enumeration or actor fields.

When a field is made hidden because of a change to a controller field, changes to that field's value since it was last saved are reverted to its original value.

Note: An exception exists for changes to values in grid and card relationship fields. The values cannot be reverted because they are saved immediately.

On the JSON tab, visible and hidden rules are defined when *type* is set to **visible** or **hidden**. You must specify either a *controllers* or *controllerName* attribute. For more information, see “[Defining Editable and Read Only rules](#)” on page 319.

In the following steps, select **Visible** or **Hidden** in **Rule Type**.

Procedure

1. In the View Designer, click the **Design** tab.
The palette is displayed.
2. Select the field that you want to add a rule to.
3. In the property panel, click **New Rule**.
4. Select a **Rule Type**.
5. In **Controlled By**, choose **One field with any value** or **Multiple controllers or values**.
6. If you choose **One field with any value**:
 - a) Select a **Controlling Field**.
 - b) Click **Done**.
7. If you choose **Multiple controllers or values**:
 - a) In **Controlling Field Logic** select **All controlling field conditions must be met** or **Any controlling field condition may be met**.
 - b) Click **New Controller**.
 - c) Choose a field in **Controlling Field**. All available controlling fields are displayed. The next selections depend on the field type.
 - For actor fields, you can set **Match Current User** and/or select other users or user groups in **Other Users or Groups**. Any match on either field resolves the controller to true. If **Match Current User** is set to true, the signed on user must be the user or be in a user group for the value in the **Controlling Field**.
 - For enumerated type fields, click **Values** and you can choose one or more individual values.
 - Click **Done**.
 - d) Click **New Controller** to add the next controller field. Repeat the previous steps until all controller fields are added. Although you can change the order of the controller fields, it has no effect in the view.
8. Click **Done**.

Defining Required rules

The **Required** rule type makes a field required depending on the value or values of one or more controller fields in a view.

About this task

The field is validated to make sure that it has a value any time a change is made to the field or one of its controller fields. If the field is required but is missing a value, a message is displayed on the field and the **Save** button is disabled.

This rule can be defined on any field type, except on relationship fields where the object type (*objectTypeName* in JSON) is set to **SOXDocument**.

If a required field dependency is already defined on a field, you cannot define additional rules of this type on that field in a Task or Creation View.

The controllers must be either enumeration or actor fields.

On the JSON tab, a required rule is defined when *type* is set to **required**. You must specify either a *controllers* or *controllerName* attribute. See “[Defining Editable and Read Only rules](#)” on page 319 for more details.

In the following steps, select **Required** in **Rule Type**.

Procedure

1. In the View Designer, click the **Design** tab.
The palette is displayed.
2. Select the field that you want to add a rule to.
3. In the property panel, click **New Rule**.
4. Select a **Rule Type**.
5. In **Controlled By**, choose **One field with any value** or **Multiple controllers or values**.
6. If you choose **One field with any value**:
 - a) Select a **Controlling Field**.
 - b) Click **Done**.
7. If you choose **Multiple controllers or values**:
 - a) In **Controlling Field Logic** select **All controlling field conditions must be met** or **Any controlling field condition may be met**.
 - b) Click **New Controller**.
 - c) Choose a field in **Controlling Field**. All available controlling fields are displayed. The next selections depend on the field type.
 - For actor fields, you can set **Match Current User** and/or select other users or user groups in **Other Users or Groups**. Any match on either field resolves the controller to true. If **Match Current User** is set to true, the signed on user must be the user or be in a user group for the value in the **Controlling Field**.
 - For enumerated type fields, click **Values** and you can choose one or more individual values.
 - Click **Done**.
 - d) Click **New Controller** to add the next controller field. Repeat the previous steps until all controller fields are added. Although you can change the order of the controller fields, it has no effect in the view.
8. Click **Done**.

Defining Greater than, Greater than or equal, Less than, Less than or equal, and Equal rules

The **Greater Than**, **Greater than or equal**, **Less than**, **Less than or equal**, and **Equal** rule types validate the value of a field and make sure that it satisfies the condition applied by the rule type. The rule can be set up to compare a field’s value with the value of another field of the same type, or with a value defined in the rule itself.

About this task

Any time a change is made to the field it is validated to make sure that it satisfies the condition. If the value is being compared to another field, it is validated any time that field’s value changes. If the condition is not satisfied, a message is displayed on the field and the **Save** button is disabled. The message explains how to provide a valid value.

These rule types can be set up on integer, decimal, date, and currency fields. When comparing two fields, both fields must be of the same type. If one of the fields has no value, the rule is not evaluated.

Text fields can also have an Equal rule, but only to compare against another text field.

On the JSON tab, comparison rules are defined when *type* is set to greater, greaterEqual, less, lessEqual, or equal. A *compareTo* attribute must also be specified.

Procedure

1. In the View Designer, click the **Design** tab.
The palette is displayed.
2. Select the field that you want to add a rule to.
3. In the property panel, click **New Rule**.
4. In **Rule Type**, choose **Greater Than**, **Greater than or equal**, **Less than**, **Less than or equal**, or **Equal**.
5. In **Compare To**, the field type determines the options.
 - For integer, decimal, and currency fields, you can choose **A specific value** and enter a value. Do not include quotation marks, decimal separators, currency codes, or symbols.
 - For integer, decimal, currency, date, and text fields, you can choose **Another field** and select a field. Only fields in the view and of the same field type are listed.
 - For currency fields, values are compared using the base amount rather than the local amount. This allows values to be compared across different currency codes.
 - For date fields, you can compare the value to today and optionally add an offset in days.
- Because the value of **Today** changes as time progresses, rules that compare against **Today** are evaluated only when a user selects a value for the field. This prevents previously saved data from failing validation due to the changing nature of **Today**.
6. Apply a **Severity** (optional). For information, see [“Controlling error severity on rules” on page 324](#).
7. Click **Done**.

Defining Minimum Length and Maximum Length rules

The **Minimum Length** and **Maximum Length** rule type validates the length of a text field or, if used together, defines a range.

About this task

The field is validated to make sure that the length of the text value is valid any time a change is made to the field. If the condition is not satisfied, a message is displayed on the field and the **Save** button is disabled. The message states how many characters are allowed.

These rules can be set up only for text fields.

You can provide either the **Minimum Length** or **Maximum Length** rule type. You can apply both to define a range.

On the JSON tab, minimum and maximum rules are defined when *type* is set to *minLength* or *maxLength*. Specify *compareTo* as a number of characters within quotation marks.

Procedure

1. In the View Designer, click the **Design** tab.
The palette is displayed.
2. Select the field that you want to add a rule to.
3. In the property panel, click **New Rule**.
4. In **Rule Type**, choose **Minimum Length** or **Maximum Length**.
5. Enter the number of characters.
6. Apply a **Severity** (optional). For information, see [“Controlling error severity on rules” on page 324](#).
7. Click **Done**.

Defining Pattern rules

The **Pattern** rule type validates that a text field has a specified format.

About this task

The field is validated to make sure that the value has the correct format any time its value is changed. If the format is not correct, a message is displayed on the field and the **Save** button is disabled.

This rule can only be set up for text fields.

On the JSON tab, a pattern rule is defined when *type* is set to **pattern**. Specify *compareTo* as a valid regular expression.

Procedure

1. In the View Designer, click the **Design** tab.
The palette is displayed.
2. Select the field that you want to add a rule to.
3. In the property panel, click **New Rule**.
4. In **Rule Type**, choose **Pattern**.
5. In **Pattern**, enter a valid regular expression, for example, `^[\d]{3}-[\d]{2}-[\d]{4}$`.
6. Apply a **Severity** (optional). For information, see “[Controlling error severity on rules](#)” on page 324.
7. Click **Done**.

Controlling error severity on rules

Use the **Severity** property to control whether errors or warnings are issued when users enter values that do not pass validation rules.

About this task

When users enter values that do not pass a field's validation rules, an error is issued and the object cannot be saved. However, if you apply the **Severity** property, warnings are issued rather than errors. When a warning is issued, an object can still be saved.

You can add a **Severity** property to any validation rule type (**Greater Than**, **Greater than or equal**, **Less than**, **Less than or equal**, and **Equal**). You can specify it to be an error, warning, or information. If a rule has no severity property, errors are issued.

For example, a warning can be issued if a date field is not within the next 90 days. If the *severity* property is omitted, an error is issued.

The text in the message is set by the system and cannot be customized.

Multiple warning messages can be displayed for a field. However, only one error message is displayed.

Conditions, for example, field dependencies and field attributes, always issue errors rather than warnings.

An information message behaves like a warning but is displayed with an information symbol. The error message text is the same whether it is a warning or an information.

On the JSON tab, specify *severity* as **error**, **warning**, or **info**.

Procedure

1. In the View Designer, click the **Design** tab.
The palette is displayed.
2. Select the field that you want to add a rule to.
3. In the property panel, click **New Rule**.

4. In **Rule Type**, choose a rule type.
5. In **Severity**, choose **Error**, **Warning**, or **Info**.
6. Click **Done**.

Chapter 15. Configuring GRC Calculations

Use the GRC Calculations feature to automatically set values on fields when an object is created, calculation input fields are updated, object associations are made, or a **run a calculation** workflow action starts.

Setting up GRC Calculations

Configure GRC Calculations so that calculations can be used in OpenPages.

About this task

During the configuration process, complete the following tasks to prepare for implementing GRC Calculations in OpenPages.

Procedure

1. Update the permissions for role templates for administrators who are configuring the calculations.

- a) Click  > **Users and Security** > **Role Templates** > role template > **Role Permissions**.
- b) Select the **SOX** > **Administration** > **Calculation** permission.

Administrators with this permission enabled can define calculations by using  > **Solution Configuration** > **Calculations**. They can also access and run calculations from **Calculations**.

2. Review the registry settings that apply to calculations. They are located in the **Platform** > **Calculation** registry settings folder.

Especially review:

- **Enabled**

Calculations are enabled (true|false).

- **Always Recalculate on the Object Save**

Recalculate object fields on the save operation all the time (true|false). If false, object fields are recalculated only when the input fields are updated.

The following registry settings control concurrent jobs and how asynchronous processing is handled: **Async Enabled**, **Async Polling Period**, **Async Queue Builder Only**, and **Concurrent Calculation Jobs**.

The **Enable Calculation Preview** setting controls whether the projected result of a calculation is displayed in views while users are editing the fields that are used by the calculation. The default value is true. You might want to change the setting to false to troubleshoot a calculation, for example.

Additionally, the **Platform** > **Processes** > **Bulk run calculations** > **Transaction Timeout** registry setting is used when an administrator runs a calculation. For more information, see [“Running a calculation as an administrator” on page 364](#).

3. Optional: Customize the content of email notifications that are sent when an administrator runs a calculation. You can use the default email template or customize the text to meet your requirements. For more information, see [“Customizing email notifications for GRC Calculations” on page 366](#).
4. Define, test, and implement calculations. For more information, see [“Defining a calculation” on page 338](#).

What to do next

Complete the following postrequisites:

- Review the Task Views. Review whether input fields and set fields are displayed in the Task Views so that you understand how users experience calculations and calculated values. For more information, see “Defining a Task View” on page 268.
- Review the GRC Workflow feature in OpenPages. Review what workflows are setting field values. For more information, see “Defining a workflow action that sets fields” on page 420.

Calculation fundamentals

The GRC Calculations feature is based on calculation definitions.

Calculations are defined by using the  > **Solution Configuration** > **Calculations** task. After you publish a calculation, it is available in OpenPages.

Show me how

This video shows you how to use the **Calculations** task. It explains the fields in a calculation definition and how a list of operations is constructed.

<https://youtu.be/0MZy60Clr-U>

Calculation definitions

A calculation definition is defined for one object type. An object type can have multiple calculations.

A calculation definition has the following characteristics:

- A calculation definition is static.
- A calculation definition is versioned.

Each time a calculation definition is published, a new version of that calculation definition is made available to users. The new version is used for object changes that are made after it is published. It does not affect calculations that have already been run.

- A calculation definition can be disabled.

When a calculation definition is disabled, no new calculation can be run. Disabled calculation definitions can be re-enabled.

A calculation definition is made up of the following elements:

- Calculation properties

Calculation properties define basic information, for example, the object type that the calculation applies to and whether the calculation is enabled.

- Applicability conditions

Applicability conditions restrict the calculation to objects that meet specific criteria.

- Operations

Operations determine what the calculation does.

Goal of a calculation

The goal of a calculation is to set a value for one or more fields on an object, based on the values of one or more other fields. Only fields on the object type for the calculation can be set. Fields on related object types cannot be set.

Important: Calculations have no effect on locked objects.

Operations determine what a calculation does

A calculation is made up of multiple operations. A calculation can have three types of operations:

- Input field operation
Retrieves an input field that is used in a later operation. An input field operation can be from the current object, a related object, or the Preference object. Conditions can be defined on the input field. A calculation can have multiple input field operations.
- Variable operation
Contains an intermediary value that is used in a later operation. A variable operation contains an expression that can use all previously defined operations, be they input fields, other variables, or set field operations. A calculation can have multiple variable operations.
- Set field operation
Sets a field value on an object. A set field operation contains an expression that can use all previously defined operations, be they input fields, variables, or other set field operations. A calculation can have multiple set field operations.

Operations are defined for a single calculation. They cannot be shared among multiple calculations.

What does the calculation type do?

The calculation type determines whether a calculation can be started by a workflow. There are two calculation types:

- Manual calculations are started only by a **run a calculation** action in a workflow.
- Automatic calculations are started in all other ways except by a **run a calculation** action in a workflow.

In Task Views, fields that contain the result of an automatic calculation are read only and cannot be changed by the users. However, fields that contain the result of a manual calculation are not read only and the values can be changed by users.

When do calculations run?

A calculation runs when an enabled, published calculation exists for an object type. An object must meet both a calculation's applicability and conditions on the value of the input field, if defined.

Manual calculations run when a **run a calculation** action in a workflow starts.

Automatic calculations run when the following actions take place:

Note: In the following list, "input field" means any field that provides input to the calculation, including (but not limited to) fields that are defined in input field operations.

- A user updates a calculation's input field on an object in a Task View.
- On a related object in a Task View, a user updates a calculation's input field. If a user updates a field on, for example, a child object, a calculation on a parent object type is run.
- A user associates an existing related object to another object, where either or both objects contain a field that is used in a calculation.
- A user starts a workflow that creates an object for an object type that has a calculation.
- A user completes a stage in a workflow that updates a calculation's input field.
- A user completes a stage in a workflow that updates a calculation's input field on a related object.
- A user completes a stage in a workflow that associates an existing related object to another object, where either object contains an input field that is used in a calculation.
- An administrator runs a calculation by clicking  > **Solution Configuration** > **Calculations**, selecting a single calculation, and clicking .
- An administrator uploads data with FastMap. The data contains new objects or changes to a calculation's input fields.
- Data is loaded by using an API, where the data contains new objects, changes to a calculation's input fields (on the object or related objects), or changes to object associations.

When a user updates an input field on an object in a Task View, all calculations for that object type that use the changed input fields are run. The order in which the calculations run cannot be defined.

New calculations and existing objects

When you create a new calculation, it does not automatically run on existing objects. A calculation is run when actions described in [“When do calculations run?” on page 329](#) take place.

Object types and calculations

An object type can have multiple calculations. But each calculation must set different fields. No two calculations can set the same field. A calculation runs for all objects that qualify for it, given the applicability and input field conditions.

Debugging calculations

For information about correcting calculations that have errors, see [“Testing and debugging a calculation” on page 365](#).

Sample calculations

OpenPages includes sample calculations. For more information, see the *IBM OpenPages with Watson Solutions Guide*.

Comparison of calculations and triggers

The GRC Calculations feature, together with the GRC Workflow feature, provide a powerful platform that allows organizations to tailor the system to their specific requirements. Existing OpenPages customers that use triggers can make a plan to transition from triggers to GRC Calculations and GRC Workflow.

Calculations can replace the following functionality that was previously available in triggers:

- Automation for data input
- Mathematical operations
- Assessment rating assignments
- Data aggregation
- Helper links

Calculations and workflows that are defined by using GRC Calculations and GRC Workflow are easier to define and maintain than triggers. Triggers require a high level of technical expertise, whereas most calculations and workflows can be defined by business specialists. For complicated calculations and workflows, technical expertise is an advantage.

Triggers that currently work in your environment, continue to work. But your organization should make a plan to transition existing triggers to calculations.

Functionality that is available in triggers is also available in GRC Calculations and GRC Workflow.

GRC Calculations FAQs

The following list provides answers to frequently asked questions about calculations.

Can one calculation set values for multiple fields?

Yes. A single calculation can set the values for multiple fields. They must be fields on the object type that the calculation is defined for.

Can multiple calculations set a value for the same field?

Yes. A field can be used as a set value operation in multiple calculations. However, the order in which calculations run is not guaranteed. Therefore, plan your calculations to avoid collisions and overwrites.

Can a calculation set a value for the same set value field multiple times within that calculation?

Yes. A value can be set multiple times for the same field within a calculation (this means that multiple set field operations for the same field are allowed).

Are there fields that a calculation is not allowed to set?

Yes. A calculation is not allowed to set the values for computed fields, workflow system fields, and many of the system fields like System Fields:Creation Date. Additionally, calculations cannot set fields that are defined as relationship fields in Task Views.

Can a calculation set user and date system fields?

No. While a calculation can use the user and date system fields as input fields, a calculation cannot set the value of the following system fields:

- System Fields:Created By
- System Fields:Last Modified By
- System Fields.Last Modification Date
- System Fields.Creation Date
- System Fields:Name

If you create your own user field and want to set it to the value in, for example, System Fields:Last Modified By, be sure to define the user field with field type defined as simple string and display type as user selector.

Can a calculation set a field that is defined as read-only in a Task View?

Yes.

Do calculations honor field dependency rules?

No. For example, if a user updates the value of an input field on a Task View and a calculation runs, the object can be saved even if the output field value does not meet the field dependency rules.

What happens if a calculation updates a controlling field?

Use caution when defining calculations that set values for fields that are controlling fields. In some situations, changes can be lost in Task Views because a loop is created. For example, say that Field B is a controlling field and Field A is a dependent field (is set to Read-only or Editable based on Field B). If a calculation updates Field B based on a change to Field A, the update to Field A might be lost in the Task view. The dependency is enforced without saving the updated value.

To avoid this, use separate Task Views, one that runs a calculation and one that sets dependent fields.

Do calculations honor dependent pick list rules if a calculation is based on the controlling field ?

Yes. If a calculation sets a value for a field that is a controlling field in a dependent pick list, it also sets values for dependent fields to allowed values.

Can a calculation set a field on a related object or Preference object?

No. A calculation can set a field only on objects of the object type that the calculation is defined for.

Can a calculation be based on a field on a related object or Preference object?

Yes. A calculation can use fields on a related object or Preference object as input fields.

How do I use Preference objects in calculations?

Preference objects specify variable values that are specific for a business entity. You can use the field values of Preference objects in calculations.

- Calculations do not use Preference Group objects. They use only Preference objects.
- The Preference object that is used is the one that is associated with the Primary Business Entity parent (or ancestor) that is closest to the object where the calculation is occurring.
- The Preference objects of non-primary business entities are not used in calculations.
- When a primary parent business entity has multiple Preference objects, you can use all of the Preference objects that are associated with the primary parent business entity. Design your calculations to handle multiple Preference objects. For example, your calculation might use a specific Preference object based on the value of a field.

Note: Some of the sample calculations that are provided with OpenPages are not designed to manage multiple Preference objects for business entities. When you run one of these sample calculations, you might get an error such as Invalid field assignment.

- If you change the field values of a Preference object or if you change the relationship of a preference object, the calculations might not run automatically.

For example, if you update a field value in a Preference object, add a Preference object, or change the primary parent of a Preference object, the calculations that use the Preference object might not run automatically. In this case, re-run the calculation. See “[Running a calculation as an administrator](#)” on page 364.

Can one calculation be linked to another calculation?

No, each calculation is independent. But the result of one calculation can cascade to other calculations. For more information, see “[Designing a calculation](#)” on page 333.

Can I include a filter within a calculation?

Yes, a filter (condition) can be applied to input fields that are defined for related objects and Preference objects.

Can a calculation get invoked from a workflow?

Yes, if the workflow starts an action that causes a calculation to run. This might include creating an object, updating an input field on an object, updating an input field on a related object, and associating objects.

Can I access siblings on a calculation?

No. Fields from siblings of the open object cannot be used as input fields.

Can I access child, parent, ascendent, and descendant objects?

Yes, input fields can be fields from child, parent, ascendent, or descendant objects.

Can a calculation invoke an association or copy operation?

No. A calculation can only set field values.

Can a calculation access the values in registry settings?

Yes

Are there sample calculations?

Yes. See the *IBM OpenPages with Watson Solutions Guide*.

Can I access a specific value in a multi-value field?

Yes. Use an index on the field, for example, at([\$Causal Category\$], 2), to access the enumerated value in the third position of the Causal Category field. It accesses the third position because counting begins at zero.

Can I edit the text in the body of the email that is sent to the administrator after they run a calculation?

Yes. The body text is defined in application text.

Is there an undo for a calculation?

No.

Can calculations be included in the scheduler?

No.

Can calculations be started by a workflow action?

Yes. Manual calculations can be started by a **run a calculation** operation on a workflow action. For more information, see “[Defining a workflow action that runs a calculation](#)” on page 425.

Can I schedule a calculation to run in off hours?

No. However, you can disable calculations all together or disable individual calculations to control when calculations run. For example, you can disable calculations before a Fast map load. Then, run the calculations after the data is loaded. You can also disable calculations during working hours. Enable the calculations, run them in off hours, and disable them again during working hours.

Must the input fields and set fields be included in a Task View for a calculation to run?

No. Calculations are run when an input field is changed, regardless of whether it is shown in a Task View or not. If the input field is required, it must be in the creation view.

When I use a Task View, what causes a calculation to run?

A calculation runs either when an object is saved or only when an input field that is used in a calculation is changed. The **Always Recalculate on the Object Save** registry setting controls the behavior.

Why are set fields updated BEFORE I click Save in a Task View?

When you change an input field and move the focus outside the field, all the calculations that use that input field are run in preview mode. The new values for set fields are calculated and displayed if they are included in the Task View. The values that are shown in preview mode are saved to the database when you click **Save**.

Do I need to click Save for the calculation to run?

No. Calculations run in preview mode when you move the focus outside an input field whose value you changed. But you must click Save for the results of the calculation to be saved in the database.

Can I manually update the value in a set field in a Task View, thereby overriding the calculated value?

It depends on the calculation type. Set fields that are calculated by automatic calculations are read only in a Task View. If the calculation is disabled, the set field becomes editable or however the field is defined to display in the Task View. Set fields that are calculated by manual calculations are not read only in a Task View and are editable.

What can I do to optimize speed and performance?

Keep the expressions as simple and short as possible. A calculation with many operations with complex expressions might impact performance.

Designing a calculation

Designing a calculation involves knowing what you expect the calculation to achieve, understanding the input fields and field values, the field value that is set, and understanding what is possible in the calculation expression.

Know what objects the calculation applies to

A calculation can run for all or selected objects of an object type.

If a calculation is run for only selected objects, the applicability and input field conditions on the calculation define the selection criteria.

Part of testing a calculation is to verify that the applicability and input field conditions are defined correctly.

Know the calculation result

Know what you want the calculation to achieve.

Know whether the calculation is started by a workflow

Calculation type (automatic or manual) determines whether a calculation can be started with a **run a calculation** action in a workflow.

Understand the operations in a calculation

Understand the operations in a calculation.

Use input fields and variables in a calculation. It makes the calculations modular and easier to debug.

Add comments to the expression.

Follow good programming practices.

Study the Loss Event calculation to see how the result of one set field operation can be used in subsequent operations.

Understand the calculation expression

Understand the possibilities available in the calculation expressions. For more information, see “[Expressions in GRC Calculations](#)” on page 342.

Understand how a calculation can cascade to other calculations

Each calculation is independent, but the result of one calculation can cause a cascade effect to other calculations.

Cascading calculations are allowed across different objects, but not on the same object.

The following example illustrates how this works:

1. A change is made to Input Field A that is used in Calculation A, which sets Set Field A to a value.
2. Set Field A is an input field that is used in Calculation B. When Set Field A changes, Calculation B runs. Calculation B sets Set Field B to a value.
3. Set Field B is an input field that is used in Calculation C and Calculation D. When Set Field B changes, Calculation C and Calculation D run. Calculation C sets Set Field C to a value. Calculation D sets Set Field D to a value.
4. The calculation can continue this pattern.

Understand how the design of the calculation can affect performance

A calculation automates object field assignments while it creates or updates objects, or after end user operations that run asynchronously. As a result, a simple object field update might trigger hundreds of subsequent object updates behind the scenes, causing a reduction in overall system performance.

Use the following techniques to manage the performance of calculations:

- Reduce the number of objects to be recalculated.

At the end of a user operation, the calculation determines whether any other objects are impacted by the change. To determine whether other objects are impacted, OpenPages looks up the related object reference in reverse order. The more objects that are identified, the more performance is affected.

When you have ancestor or descendant references, the reverse lookup might identify hundreds of objects. Consider the following techniques:

- Use the **Applicability** condition to limit the number of objects to be recalculated.
- When setting up an operation on an input field in a related object, apply **Filter By** conditions to a **Related Object Field**.
- When setting up an operation on an input field in a related object, where the **Relationship Type** is **Direct Parent**, enable **Primary Parent Only**.
- Understand the impact of chaining calculations.

You can define calculations so that they can depend on other calculations recursively and the calculation can identify all the impacted objects and recalculate values in sequence. However, the performance impact to the overall system of such a chain of calculations can be substantial.

The following sequence of events is an example of a chain of calculations:

1. You have a calculation that updates an Action Item.
2. The update to the Action Item causes a calculation to update the Issue Status of the parent Issue.
3. The Issue Status is used to classify the parent Control object.
4. The Classification of the Control is used to calculate the Audit Inherent Risk Rating of the parent Risk.
5. The Audit Inherent Risk Rating of the Risk is aggregated on the parent Process.

While you are developing a calculation, do the following:

- Monitor the "In queue" count column on the calculations administrative page.
- Update an object as a test.
- Refresh the calculations page periodically to see the impact of the object update.

If you see a spike on the "In queue" count on some calculations, analyze the chain relation and optimize the calculation definitions.

- Understand how the automatic update of workflow assignees can slow performance.

When a workflow assignee definition is set to an object field and that field is updated on the object, the workflow assignee is updated automatically. The automatic assignee update uses the same engine as calculations do. The asynchronous processing shares the queue to manage the recalculation of object fields and workflow fields. As the queue grows, both calculations and workflow auto updates get slower.

- Set the cache size high enough to keep workflows in the on-memory cache.

Often there are many active workflows that spread across multiple versions of workflow definitions. OpenPages tries to read workflow definitions to find impacted workflows. If the workflows are not available in the on-memory cache, OpenPages gets the workflow definitions from the database.

Create the registry setting **Platform > Workflow Implementations > OP > Expired Process Definition Cache Size** and set it to a positive integer value. To avoid degraded performance, do not set this value lower than the default value of 200. For more information about creating a custom setting, see ["Creating a custom setting" on page 499](#).

- Terminate workflows that are no longer in use because they can take up resources. Unused workflows are especially common in a development environment.
- Don't use calculations with custom triggers on the same object.

It is technically possible to use calculations and custom triggers on the same object. However, this practice can cause multiple calls to the database for a single user operation, and debugging custom trigger code can be difficult. Most tasks can be accomplished with calculations or workflows. For example, you can use a calculation for auto field assignment instead of custom triggers.

- Tune the calculation configuration registry settings.

There are several registry settings that you can use to control the performance of calculations.

- If you increase the value of **Platform > Calculation > OP > Concurrent Calculation Jobs** to increase throughput of asynchronous processing of the calculations, it might limit computation resources for other user activities on the OpenPages system.
- You can set **Platform > Calculation > OP > Always Recalculate on the Object Save** to **true** during the development phase of a calculation to easily see the calculation result after the calculation definition update. However, it results in redundant recalculation in a production system where the calculation definition is not changed frequently.
- If you increase the value of **Platform > Calculation > OP > Task View Timeout for Queued Object**, it can have an impact on performance. When an object is opened in Task View, OpenPages displays a waiting icon for each object field with calculations in the queue. This icon is displayed until the results become available or the number of minutes specified in **Task View Timeout for Queued Object** have elapsed. While the waiting icon is displayed, OpenPages keeps using the server-side resources to monitor the progress of the calculation. The larger the value of this setting, the more it can impact the overall performance of your OpenPages system.

Keep it simple

Calculations that have many operations that have complex expressions can impact performance. Avoid making a calculation overly complicated. Keep the expressions as short and simple as possible.

Common calculation use cases

Study the use cases to learn how to write calculations for common scenarios you might encounter.

- Use case 1: Set a value on a parent object that is the sum of values on child objects
- Use case 2: Set a date on a parent object based on dates from child objects
- Use case 3: Set an enumerated value based on other enumerated values

Use case 1: Set a value on a parent object that is the sum of values on child objects

In this use case, you want to set Estimated Gross Loss on Loss Event parent objects to the sum of Estimated Loss on the child Loss Impact objects. The calculation is defined for the Loss Event object type. The two fields that are involved are OPSS-LossEv:Estimated Gross Loss on Loss Event objects and OPSS-LossIm:Estimated Loss on Loss Impact objects.

The Estimated Loss operation gets the values of the OPSS-LossIm:Estimated Loss field from the child Loss Impact objects.

Table 112. Use Case 1: Estimated Loss operation				
Operation Name	Type	Object Type	Field	Reference type
Estimated Loss	Input Field	LossImpact	OPSS-LossIm:Estimated Loss	Direct Child

The Set Estimated Loss operation sums the values of the OPSS-LossIm:Estimated Loss field from the Estimated Loss operation and sets the value of OPSS-LossEv:Estimated Loss on the parent object to the sum or to zero.

Table 113. Use Case 1: Set Estimated Loss operation			
Operation Name	Type	Output Field	Expression
Set Estimated Loss	Set Field	OPSS-LossEv:Estimated Loss	if exists (SUM ([\\$Estimated Loss\$])) then SUM ([\\$Estimated Loss\$]) else currency(0.00, 'USD') endif

Use case 2: Set a date on a parent object based on dates from child objects

In this use case, you want to set a Due Date on a parent Issue to the most recent due date on child Action Item objects. The calculation is defined for the Issue object type. The two fields that are involved are OPSS-AI:Due Date on Issue objects and OPSS-AI:Due Date on Action Item objects.

Table 114. Use case 2: GetDate operation				
Operation Name	Type	Object Type	Field	Reference type
GetDate	Input Field	SOXTask	OPSS-AI:Due Date	Direct Child

Table 115. Use Case 2: Set Date operation			
Operation Name	Type	Output Field	Expression
SetDate	Set Field	OPSS-Iss:Due Date	max ([\\$GetDate\$])

Use case 3: Set an enumerated value based on other enumerated values

In this use case, you want to set Criticality on Asset objects to values from Confidentiality, Integrity, and Availability on the same object. The calculation is defined for the Asset object type.

The first three operations get the values of the OPSS-CIA:Confidentiality, OPSS-CIA:Integrity, and OPSS-CIA:Availability fields on an Asset object.

Table 116. Use Case 3: the three Input Field operations				
Operation Name	Type	Object Type	Field	Reference type
C	Input Field	Asset	OPSS-CIA:Confidentiality	Self
I	Input Field	Asset	OPSS-CIA:Integrity	Self
A	Input Field	Asset	OPSS-CIA:Availability	Self

The Set Criticality operation sets the value of OPSS-CIA:Criticality based on the values of the three preceding operations.

Table 117. Use Case 3: Set Criticality operation			
Operation Name	Type	Output Field	Expression
Set Criticality	Set Field	OPSS-CIA:Criticality	If ([C\$] == 'High' OR [I\$] == 'High' OR [A\$] == 'High') then 'High' elif ([C\$] == 'Medium' OR [I\$] == 'Medium' OR [A\$] == 'Medium') then 'Medium' elif ([C\$] == 'Low' OR [I\$] == 'Low' OR [A\$] == 'Low') then 'Low' else 'Not Available' endif

Managing calculation definitions

The **Calculations** task is used to define, publish, and manage calculations.

To manage calculations, click  > **Solution Configuration** > **Calculations**. Whether the menu item is displayed depends on your access permissions.

Calculation List

When you click  > **Solution Configuration** > **Calculations**, a Calculation List is displayed.

From the Calculation List, you can:

- Click a calculation. The calculation definition opens and you can view or make changes to it.

- Click the **Name** column header to change the sort order of the list.
- Select the check box next to a single calculation or multiple calculations to update numerous calculations. The bulk update options are:
 - Enable
 - Disable
 - Delete
 - Run
- Select the check box next to a single calculation and click **Run ▶** to run a calculation for numerous objects at once. For more information, see “[Running a calculation as an administrator](#)” on page 364.
- Click **New Calculation** to create a new calculation. For more information, see “[Defining a calculation](#)” on page 338.

How to save a calculation

Your work is automatically saved as you define a calculation.

How to publish a calculation

Click **Publish** when the calculation is finished.

Each time a calculation definition is published, a new version of that calculation definition is made available.

How to discard a draft version of a calculation

To discard changes you made to a calculation, click **Discard Draft**. All changes since the last published version are discarded.

How to disable a calculation

To disable a calculation, select a calculation from the Calculation List. Select **Disable**.

How to work on a calculation as a team

When you have a calculation definition open, the URL contains the calculation's internal name. If you are working on the calculation with colleagues, you can send them the URL to share your progress. Although you can collaborate with colleagues, only one user should work on a calculation at a time.

Defining a calculation

A calculation definition contains basic information, applicability, and operations.

About this task

The main parts of a calculation are the operations and the expressions. Operations determine what the calculation does:

- At a minimum, one **Set Field** operation is mandatory.
- A calculation can optionally have multiple **Input Field** operations and multiple **Variable** operations.
- The operations are processed in the order listed. The operations can be reordered.
- Place the **Set Field** operations last in the list.
- An expression must be valid and free of syntax errors to save an operation.

Tip: If you are having trouble getting the syntax correct for an expression, provide a dummy expression like 1+2 so that you can save the operation and not lose your work if the session times out.

Procedure

1. Click  > **Solution Configuration** > **Calculations**.

2. Click **New Calculation**.

3. Enter an internal **Name** for the calculation.

Allowed characters are A-Z, a-z, 0-9, underscore, hyphen, and spaces. Special characters are not allowed.

4. Enter a **Description**.

Note: For complicated calculations, provide a short statement that describes each operation. This ensures that anyone who follows you can understand and debug the calculation.

5. Leave **Enabled** selected. It can be changed later.

6. Select an **Object Type**. It cannot be changed later.

7. Select Manual or Automatic in **Calculation Type**.

- Manual calculations are started only by a **run a calculation** action in a workflow.
- Automatic calculations are started in all other ways except by a **run a calculation** action in a workflow.

8. Click **Create**.

The window expands. The word *Draft* and the version number, 1, are displayed next to the calculation name. You can begin defining the calculation.

9. In **Applicability** you define the conditions for the calculation. Expand **Applicability** and click **New Condition**. The **Applicability** panel opens.

- Leave **Applicability** empty if the calculation runs for all objects of the object type.
- Add conditions to restrict the calculation to specific objects of the object type.
- For each condition, you build a comparison statement with two fields and an operator.
- If you define multiple conditions, all conditions must be met for the calculation to start.

To override this rule, define **Advanced Logic** to combine the conditions in a specific way.

Note: Do not use the System Comment field (System Fields:Comment) in calculations. This system field is a special field that is used with File (SOXDocument) and Signature objects.

a) In **Compare**, you define the first field in the comparison statement. You can choose:

- **A field in the current object**

Select an **Object Field**.

- **A field in a related object**

– Select Direct Child, Direct Parent, Ancestor, or Descendant in **Relationship Type**.

– Select an object type in **Related Object Type**.

– Select a field in **Related Object Field**.

– Select a path in **Relationship Paths** (displays only if **Relationship Type** is Ancestor or Descendant).

– Add **Filter By** conditions (optional).

– Set **Primary Parent Only** (displays only if **Relationship Type** is Direct Parent or Ancestor) (optional).

- **A field in a Preference object**

Select a **Preference Object Field**. You can add **Filter By** conditions.

- **End User**

An **End User** condition checks whether the signed on end user is a specified user and whether the user is in a specified user group. The second field in the comparison statement is a specified value, an expression, or an actor field on an object.

b) In **Using**, choose an **Operator**. The list of operators depends on the field type of the field you chose in **Compare**.

c) In **To**, you define the second field in the comparison statement. You can choose:

- **A specified value**

The value that you can provide depends on the field type of the field you chose in **Compare**. The comparison is case sensitive, so ensure that you specify the correct case for the value.

- **An expression**

Enter a single field or variable from the list in “[Using variables, functions, and fields](#)” on page 377. All of the variables and fields listed there can be used in an expression. The field or variable must be in the given format. It can, however, be part of a longer string, for example, a file name like Evidence_[\$Parent:SOXRisk/System Fields:Name\$].pdf if you want to validate that the parent object has a specific PDF attachment.

- **A field in the current object**

Select an **Object Field**.

- **A field in a related object**

- Select **Direct Child**, **Direct Parent**, **Ancestor**, or **Descendant** in **Relationship Type**.
- Select an object type in **Related Object Type**.
- Select a field in **Related Object Field**.
- Select a path in **Relationship Paths** (displays only if **Relationship Type** is Ancestor or Descendant).
- Add **Filter By** conditions (optional).
- Set **Primary Parent Only** (displays only if **Relationship Type** is Direct Parent or Ancestor) (optional).

- **A field in a Preference object**

Select a **Preference Object Field**. You can add **Filter By** conditions.

d) If you chose a date field in **Compare**, you can define an offset in **Adjust Date By**.

- **A specified value** and enter **Number of Days**.

- **A field in the current object**

- **A field in a related object**

- Select Direct Child, Direct Parent, Ancestor, or Descendant in **Relationship Type**.
- Select an object type in **Related Object Type**.
- Select a field in **Related Object Field**.
- Select a path in **Relationship Paths** (displays only if **Relationship Type** is Ancestor or Descendant).
- Add **Filter By** conditions (optional).
- Set **Primary Parent Only** (displays only if **Relationship Type** is Direct Parent or Ancestor) (optional).

- **A field in the Preference object**

You can add **Filter By** conditions.

e) Click **Done**.

The condition is saved and assigned a number. Conditions are numbered consecutively in the order they are defined.

- f) Optional: Add more conditions.
- g) Optional: Set **Advanced Logic** to true to override the default rule that all conditions must be met. Write a statement in **Logic**. Use the condition numbers together with the operators and, or, not, and parentheses.
The order of operations is: () then NOT then AND then OR.
- For example:
- 1 or 2 or 3
 - 1 and (2 or 3)
 - 1 not (2 or 3)
10. In **Operations** you define what the calculation does. Expand **Operations** and click **New Operation**.
The **Operation** panel opens.
11. Define **Input Field** operations for the calculation.
- a) Click **New Operation**.
 - b) In **Type**, select **Input Field**.
 - c) Enter an internal **Name** for the operation.
Allowed characters are A-Z, a-z, 0-9, underscore, hyphen, and spaces. Special characters are not allowed. The name must not start with a number or a space.
 - d) Click **Add Field**.
The panel expands and three options are displayed:
 - **A field in the current object**
 - **A field in a related object**
 - **A field in a Preference object**
 - e) If you select **A field in the current object**, select an **Object Field** and click **Done**.
 - f) If you select **A field in a related object**, complete the following fields:
 - Select Direct Child, Direct Parent, Ancestor, or Descendant in **Relationship Type**.
 - Select an object type in **Related Object Type**.
 - Select a path in **Relationship Paths** (displays only if **Relationship Type** is Ancestor or Descendant).
 - Select a field in **Related Object Field**.
 - Choose a **Field to sort on**.
 - Select Ascending or Descending in **Sort Direction**.
 An example of how you can use sorting is to list months in different orders. For example, to analyze trends, you might want to sort KRI values by January, February, and March. Then, later by March, February, and January.
 - g) If you select **A field in a Preference object**, complete the following fields:
 - Select a field in **Preference Object Field**.
 - Add **Filter By** conditions (optional). If you add multiple conditions, set **Advanced Logic** as needed.
 - Click **Done**.
 - h) Define more **Input Field** operations, as needed by the calculation.

12. Define **Variable** operations for the calculation.

- a) Click **New Operation**.
- b) In **Type**, select **Variable**.
- c) Enter an internal **Name** for the operation.

Allowed characters are A-Z, a-z, 0-9, underscore, hyphen, and spaces. Special characters are not allowed. The name must not start with a number or a space.

- d) All input fields, variables, and set fields that precede this operation are listed in **Involved Fields**.
- e) Enter an **Expression**. For more information, see “[Expressions in GRC Calculations](#)” on page 342.
- f) Click **Done**.

g) Define more **Variable** operations, as needed by the calculation.

13. Define **Set Field** operations for the calculation.

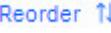
- a) Click **New Operation**.
- b) In **Type**, select **Set Field**.
- c) Enter an internal **Name** for the operation.

Allowed characters are A-Z, a-z, 0-9, underscore, hyphen, and spaces. Special characters are not allowed. The name must not start with a number or a space.

- d) Select a field in **Output Field**.
- e) All input fields, variables, and set fields that precede this operation are listed in **Involved Fields**.
- f) Enter an **Expression**. For more information, see “[Expressions in GRC Calculations](#)” on page 342.
- g) Click **Done**.

h) Define more **Set Field** operations, as needed by the calculation.

14. Review the operations.

- a) To reorder the operations, click .

Use drag and drop to set the processing order. Click **Done**.

- b) To remove an operation, click it and select **Remove**.

15. When you are ready to test the calculation, click **Publish**.

The 1 version of the calculation becomes the first published version.

16. Run the calculation to test it.

For information about correcting calculations that have errors, see “[Testing and debugging a calculation](#)” on page 365.

17. If you need to make changes to the calculation, open it again. Since you are now opening a published calculation, the word *Published* appears, the version number is displayed next to the calculation name and the **Publish** button is grayed out. When you make a change to the calculation, *Published* changes to *Draft*, the version number is incremented by 1, and the **Publish** button becomes active.

What to do next

Each time you change the calculation, you need to publish it and re-test it.

Expressions in GRC Calculations

The Set Field and Variable operations in a calculation contain an **expression**.

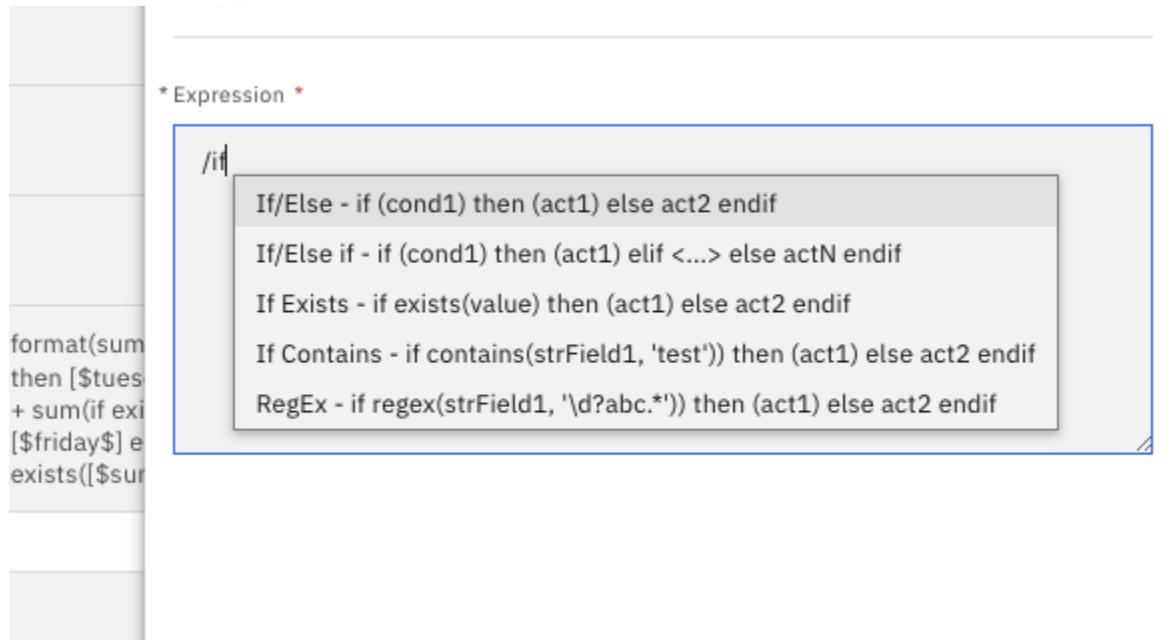
Using the content assist feature to build an expression

You can type / (slash) followed by any of the following keywords to choose from a list of all of the available expressions that relate to that keyword.

- date

- list
- currency
- if
- string

For example, if you type **/if**, you can choose from the following list of expressions:



You can type **[\$** to choose from a list of previously defined fields.

For example, given the fields shown in the following image, if you type **[\$**, you can choose from the list of fields:

Name	Field Path
monday	OPSS-Timesheet:Monday
tuesday	OPSS-Timesheet:Tuesday
wednesday	OPSS-Timesheet:Wednesday
thursday	OPSS-Timesheet:Thursday
friday	OPSS-Timesheet:Friday
saturday	OPSS-Timesheet:Saturday
sunday	OPSS-Timesheet:Sunday
total	OPSS-Aud:Actual Hours

* Expression *

[\$

- monday - [\$monday\$]
- tuesday - [\$tuesday\$]
- wednesday - [\$wednesday\$]
- thursday - [\$thursday\$]
- friday - [\$friday\$]
- saturday - [\$saturday\$]
- sunday - [\$sunday\$]
- total - [\$total\$]

] \$

As you type, the options are filtered to show only the fields that match.

Syntax rules for expressions

An expression must be written in the correct syntax.

Syntax rules:

- Numbers, dates, string values, operands, object fields, operation names, variables, and functions are allowed.
- String values must be enclosed in single or double quotation marks. For variables, such as `[END_USER]`, string values enclosed in double quotation marks are resolved, whereas those enclosed in single quote marks are kept as-is.

- Spaces are not a syntax error between operands in an entire expression, for example, between operands like + and == and in if/then/else/endif statements. Extra spaces and no spaces are allowed.
- Carriage returns (new lines) are allowed.
- Values within [\$\$] are case-sensitive. This means that the special variable, [\$END_USER\$], must be written in uppercase in an expression.
- Values outside of [\$\$] are case-insensitive. This means that the names of functions are case-insensitive, for example, sum, Sum, and SUM are all valid.
- String values that are enclosed in single or double quotation marks are case-sensitive. For example, for an if/then/else/endif statement that contains a condition like if "test" == "TEST", the result is false.
- Operation names must be enclosed in [\$\$] and be given correctly in both spelling and case. This means that an operation that is named Get Due Date is written in subsequent operation expressions as [\$Get Due Date\$].
- Object field names must be given in the following format: [\$field group:field name\$]. The field group and field name must be given correctly in both spelling and case.
- Object field names that reference parent, child, and preference objects must be given in the correct format. The object type, field group, and field names must be given correctly in both spelling and case. For example, for [\$Child:object type/field group:field name\$], the spelling and case of all names must be correct and the C in Child must be capitalized.

For more information about object fields, see [“Object fields ” on page 351](#).

- Add system variables, if needed. For more information, see [“System variables ” on page 352](#).
- Apply functions, if needed. Functions must be correct for the data type. For more information, see:
 - [“Functions for string values ” on page 353](#)
 - [“Functions for lists and numerical values” on page 354](#)
 - [“Functions for dates” on page 357](#)
 - [“Functions for currency values” on page 359](#)
- Arguments for functions must be enclosed in parentheses.
- Starting and ending parentheses must match.
- Functions that require no arguments must have empty parentheses. For example, the tomorrow function is written as tomorrow().
- A function can contain another function as an argument.
- Use if/then/else/endif statements, if needed. For more information, see [“If/then/else/endif statements” on page 360](#).
- Add comments (optional). Comments must be given in the correct format.

Operands for string values

The + operand can be used on string values.

Table 118. Operands for string values

Operand	Description	Expression	Result
+	Concatenates two or more text strings. A string value can be enclosed in either single or double quotation marks.	"abc" + "def" [\$S1\$] + [\$S2\$], where the operations contain the string values abc and def [\$S1\$] + "def" [\$field group:field name\$] + "def", where the field contains string value abc	abcdef

Operands for numerical values

The following operands can be used for integer, decimal, or currency values. Add and subtract can be used for dates. If an argument is a list, the operand is applied to all items in the list.

Table 119. Operands for numerical values

Operand	Description	Expression	Result
+	Add	100.00 + 5 [\$N1\$] + [\$N2\$], where N1 contains 100.00 and N2 contains 5 [\$N1\$] + 5 [\$field group:field name\$] + 5, where the field contains 100.00 ([\$TODAY\$] + 10), where today is May 18, 2020.	105.00 105.00 105.00 105.00 2020-05-28
-	Subtract	100.00 - 5 [\$field group:field name\$] - 5, where the field contains the date 2020-06-06 [\$L1\$] - 5, where L1 is a list of the following values: 100.00, 200.00, 300.00	95.00 2020-06-01 95.00, 195.00, 295.00
*	Multiply	100.00 * 5	500.00
/	Divide	100.00 / 5	20.00
()	Set precedence	100.00 / (2 + 3) 10 * ([\$N1\$] - 30.3), where N1 contains 100.00.	20.00 697.00

Syntax rules for comments

You can add two types of comments to an expression:

- Paragraph comments

Enclose the text in slash single or double asterisk, for example, /* text */ or /** text **/. Optionally begin each line within the block with an asterisk.

- One-line comments

- Begin a line with double slash, for example, // text
- Place the comment text after an expression, for example, [\$N1\$] + 5 // Add 5 to N1

Both types of comments are included in the following example expression:

```
/**  
 * KRI Indicator trend  
 * Calculated by comparing two KRI Value Breach Status and setting to Not Determine, Steady,  
 Worse, Better  
 **/  
//case 1: not enough KRI values  
if count([$Child:KeyRiskIndicatorValue/OPSS-KRI-Shared:Breach Status/DescB:OPSS-KRIVAL:Value  
Date$]) < 2  
// case 2: one of the recent has "Not Determine"  
elif (( at ([$Child:KeyRiskIndicatorValue/OPSS-KRI-Shared:Breach Status/DescB:OPSS-KRIVAL:Value  
Date$], 0)  
    == ( at ([$Child:KeyRiskIndicatorValue/OPSS-KRI-Shared:Breach Status/DescB:OPSS-KRIVAL:Value  
Date$], 1)  
// case 3: two recent ones have the same breach status
```

Tutorial: writing expressions

The tutorial illustrates how to write expressions in different ways.

Show me how

This video shows you how to write expressions that use integer, decimal, and currency fields. You also learn how to use parentheses for precedence and how to apply operands to lists and dates.

<https://youtu.be/CfPCYZX10AM>

Basic expressions

Let's start with some basic expressions, where the operation type is Variable.

Table 120. Examples of basic expressions

Operation name	Expression	Result	Note
N1	1 + 2	N1 is set to 3	
D1	2020-10-10 + 2	D1 is set to 2020-10-12	
S1	"abc" + "def"	S1 is set to abcdef	

Expressions that use operation names

Then, to use those operations in expressions in subsequent operations, enclose the operation name in [\$\$], as shown in the following examples:

Table 121. Examples of expressions that use operation names

Expression	Result	Note
([\$N1\$] * 2)+100	106	Where N1 contains the expression, 1 + 2

Table 121. Examples of expressions that use operation names (continued)

Expression	Result	Note
[\$D1\$] + 10	2020-10-22	Where D1 contains the expression, 2020-10-10 + 2
[\$S1\$] + [\$S2\$]	abcdefxyz	Where S1 and S2 contain the string values <i>abcdef</i> and <i>xyz</i> , respectively

Expressions that use object fields

Expressions can retrieve values from object fields, as shown in the following examples:

Table 122. Examples of expressions that use object fields

Expression	Result	Note
[\$Field Group:Number1\$] + [\$Field Group:Number2\$]	3	Where the value in <i>Number1</i> is 1 and <i>Number2</i> is 2
[\$Field Group:Date1\$] + 2	2020-10-12	Where the value in <i>Date1</i> is 2020-10-10
[\$Field Group:String1\$] + [\$Field Group:String2\$]	abcdefxyz	Where the value in <i>String1</i> is <i>abcdef</i> and <i>String2</i> is <i>xyz</i>

Expressions that mix operation names and object fields

You can mix operation names and object fields in an expression, as shown in the following examples:

Table 123. Examples of basic expressions that mix operation names and fields names

Expression	Result	Note
[\$N1\$] * [\$Field Group:Number3\$]	300	Where <i>Number3</i> contains 100.
[\$D1\$] + 10	2020-10-22	Where [\$D1\$] contains the expression, 2020-10-10 + 2
[\$S1\$] + [\$Field Group:Description\$]	<i>abcdef</i> <i>Description value</i>	Where [\$Field Group:Description\$] contains <i>Description value</i>

Expressions that use functions

You can apply functions to values, fields, and operations, as shown in the following examples:

Table 124. Examples of functions that are applied to values, fields, and operations.

Expression	Result	Note
<code>max(5000, 10000, 15000, 20000)</code>	20000	The <code>max</code> function finds the maximum value in a list.
<code>max ([\$Child:LossImpact/OPSS-LossIm:Estimated Loss\$])</code>	20000.00	Where four child objects contain the following values in the <code>Estimated Loss</code> field: 5000.00, 10000.00, 15000.00, 20000.00
<code>max ([\$Loss1\$], [\$Loss2\$], [\$Loss3\$], [\$Loss4\$])</code>	20000.00	Where the four operations that are given contain the following values: 5000.00, 10000.00, 15000.00, 20000.00
<code>count ([\$Child:LossImpact/OPSS-LossIm:Estimated Loss\$])</code>	4	Number of items

Working with lists

Lists are a means to access and work with multiple values for objects and fields.

Show me how

This video shows you how to work with lists. It explains how to retrieve values from related objects fields, work with multi-valued fields, create and manipulate lists, and apply functions to items in a list.

<https://youtu.be/6TPd1sXeH5k>

About lists

A common requirement for a calculation is to get values from multiple objects and do something with the list of values that is retrieved.

To get the values from multiple objects, define an Input Field operation that designates what object type and field you want to retrieve. You can optionally apply a condition to get only specific values. For more information, see [“Applying a condition to get only specific objects in a list” on page 350](#). You can also optionally sort the values in ascending or descending direction either by the chosen field or another field on the object type.

The result of such an Input Field operation is a list of values.

For example, for a calculation on the `Loss Event` object type, the `Estimated Loss` operation retrieves values in the `OPSS-LossIm:Estimated Loss` field on all child `LossImpact` objects. If there are four child objects, the result is like this:

5000.00, 10000.00, 15000.00, 20000.00

If the list were sorted in descending order, it would be:

```
20000.00, 15000.00 10000.00 5000.00
```

Expressions in subsequent operations can refer to the Estimated Loss operation and apply functions either to the entire list or individual items in the list using an index. The term *index* refers to positions in the list, where the index starts counting at zero. In the previous example, the value 20000.00 is in index position 0, 15000.00 is in position 1, and so on.

The same principle applies if an Input Field operation retrieves values from a field that contains multiple values, for example, a multi-actor field. You can optionally apply a condition to get only specific values. You can also optionally sort the values in ascending or descending direction either by the chosen field or another field on the object type.

Some functions can be applied to all items in a list, regardless of the type of data in the list. For example, the count function can be used for any list. Given the previous example, the result of the following two example expressions is 4.

```
count ([$Estimated Loss$])
```

```
count ([$Child:LossImpact/OPSS-LossIm:Estimated Loss$])
```

Some functions can be applied to lists of specific data types. For example, for a list that contains numerical values, you can use the sum, max, and min functions.

For example, a Set Field operation can contain this expression that sets Estimated Gross Loss on the parent Loss Event to sum of the results in the Estimated Loss operation:

```
if exists (SUM ([$Estimated Loss$])) then SUM ([$Estimated Loss$]) else currency(0.00, 'USD')
```

The result of the Set Field operation would be 50000.00 (20000.00 + 15000.00 + 10000.00 + 5000.00).

For a list that contains string values, you can use functions that split, join, and concatenate string values.

Some functions use the index so that you can access specific positions in the list, for example, you can use the at function to access specific items in a list. For example, if the Estimated Loss operation results in the following list:

```
5000.00, 10000.00, 15000.00, 20000.00
```

The following expression results in 5000.00, the value of the item in the first position (index position zero).

```
at ([$Estimated Loss$], 0)
```

The following expression results in 15000.00, the value of the item in the third position (index position two).

```
at ([$Estimated Loss$], 2)
```

You can also add and remove items from the list. For example, the following expression appends items to a list:

```
append( [$Estimated Loss$], 30000.00, 40000.00, 50000.00 )
```

Results in the following list:

```
5000.00, 10000.00, 15000.00, 20000.00, 30000.00, 40000.00, 50000.00
```

Applying a condition to get only specific objects in a list

You can optionally apply a condition to get only specific objects in a list. For example, say that for a calculation on Risk objects, you want to get a count of child Control objects. But you only want to

count Control objects whose Operating Effectiveness is set to Effective. Define an input field named GetControls for Control objects and specify a **Filter By** condition where Operating Effectiveness is equal to Effective. Then define an operation with the expression count ([**\$GetControls\$**]). The result is a count of Control objects whose Operating Effectiveness is set to Effective.

Setting an Output Field value when the expression result is a list

Special rules apply when an expression result is a list of values but the Set Field operation contains an Output Field that sets a single field value.

<i>Table 125. List results in expressions</i>	
When an expression result is...	Output Field is set to ...
One related object	The field value from that object
Multiple related objects but they all have the same field value	The value from the objects
Multiple related objects, where only one object has a value and the others are not set	The value from the one object
Multiple related objects, where they have different values	No value is set and a calculation error is issued.

Object fields

Object fields can be used in expressions.

Object fields are relative to the object type of the calculation and the current object, meaning the object that the calculation is processing.

<i>Table 126. Syntax for object fields</i>		
For	Use the syntax	Result
An object field on current object	[\$field group:field name\$]	The value of an object field on the current object.
A system field on the current object	[\$System Fields:field name\$]	The value of a system field on the current object.
A field on the Preference object	[\$Preference/field group:field name\$]	The value of an object field on the Preference object type.
Fields on parent objects	[\$Parent:object type/field group:field name\$]	A list of field values from parent objects, relative to the current object.
Fields on child objects	[\$Child:object type/field group:field name\$]	A list of field values from child objects, relative to the current object.
Fields on child objects and sort the list in ascending or descending order	[\$Child:object type/field group:field name/AscBy:field group:sort field name\$] [\$Child:object type/field group:field name/DescBy:field group:sort field name\$]	A sorted list of field values from child objects, relative to the current object.

The following examples illustrate how you can use object fields:

Table 127. Examples of expressions that use object fields

Expression	Result	Note
[\$Child:SOXTask/System Fields:Name\$]	Iss-11-001-AI_01, Iss-11-001-AI_02, Iss-11-001-AI_03, Iss-11-001-AI_04	Result is a list of the names of all child Action Items objects on a parent Issue object
[\$Child:LossImpact/OPSS-LossIm:Estimated Loss\$]	5000.00, 10000.00, 15000.00, 20000.00	Result is a list of estimated loss values from child Loss Impact objects for a parent Loss Event object

System variables

System variables can be used in expressions.

Table 128. System variables

System variable	Result
[\$APPLICATION_URL\$]	A URL for OpenPages.
[\$COGNOS_URL\$]	A URL for IBM Cognos Analytics.
[\$ApplicationText/application text key\$]	Application text content.
[\$TASK_VIEW_URL\$]	A URL to an object task view.
[\$System Fields:Task View URL\$]	Deprecated. Use [\$TASK_VIEW_URL\$].
[\$Setting/OpenPages/...\$]	A registry setting value.
[\$END_USER\$]	The user name of the signed on user.
[\$TODAY\$]	Today's date.
[\$DaysFromNow/field group:field name\$]	A day count from today to a given date. Requires a date field as an argument. For example: [\$DaysFromNow/OPSS-Iss:Original Due Date\$] result is 15, given that there are 15 days between today and the Issue Due Date

The following examples illustrate how you can use system variables:

Table 129. Examples of expressions that use system variables

Expression	Result	Note
[\$END_USER\$]	JSMITH	Result is the user name of the signed on user.
format ([\$END_USER\$])	Jane Smith - JSMITH	Result is <first name + last name - user name> of the signed on user.
[\$TODAY\$]	2020-11-09	Given that today's date is November 9, 2020.

Table 129. Examples of expressions that use system variables (continued)

Expression	Result	Note
<code>format ([\\$TODAY\$]+10)</code>	November 19, 2020	Given that today's date is November 9, 2020.
<code>[\$Setting/OpenPages/Solutions/PCM/Global Settings/Draft Policy Library\$]</code>	Global Financial Services	The result is the value of the Draft Policy Library registry setting, in this case, Global Financial Services.

Functions for string values

Functions for string values can be used in expressions.

Table 130. Functions for string values

Function	Description	Syntax
<code>format</code>	Result is a value that is changed to human-readable format. Valid for date, currency, and actor fields. For example, use <code>format</code> to make a date human readable so that it can then be appended to a text string. Use <code>format</code> to make an actor field human readable so that a user's name can be inserted in a text string. Do not use <code>format</code> for a date subject to an equation.	format(<i>input</i>) Example: <code>format([\\$fdGroup1:fdDate1\$])</code> or <code>format([\\$fdGroup1:fdCurrency1\$])</code>
<code>indexOf</code>	Result is the index of the first occurrence of <i>string2</i> out of <i>string1</i> . It is used to get parts of a string. If <i>string1</i> is a list, the <code>indexOf</code> function is applied to all items in the list. The result is a list of integers.	indexOf(<i>string1</i>,<i>string2</i>) Example: <code>indexOf('abcdefedcba', 'c')</code> result is 2
<code>join</code>	Joins a list of strings, where <i>delimiter</i> is a delimiter. For example, use to build a list of child action item names separated by commas.	join(<i>delimiter</i>,<i>list1</i>) Example: <code>join('-', ['a', 'b', 'c'])</code> result is a-b-c
<code>LastIndexOf</code>	Result is the index of the last occurrence of <i>string2</i> out of <i>string1</i> . If <i>string1</i> is a list, the <code>LastIndexOf</code> function is applied to all items in the list. The result is a list of integers.	LastIndexOf(<i>string1</i>,<i>string2</i>) Example: <code>lastIndexOf('abcdefedcba', 'e')</code> result is 6
<code>length</code>	Result is the length of a string value. For example, if you know the length, you can use it in an expression to remove part of a string. If <i>string1</i> is a list, the <code>length</code> function is applied to all items in the list.	length(<i>string1</i>) Example: <code>length('abcdef')</code> result is 5

Table 130. Functions for string values (continued)

Function	Description	Syntax
substring	<p>Result is a portion of a string. The portion can either be from a given start index position to the end of the string or from given start and end index positions. Can have one or two arguments. If one argument is given, the result is a string value from the given index position to the end of the string. If two arguments are given, result is the portion of a string between the index positions. For example, if a unique identifier is part of an object name that was assigned using autonaming, use substring to extract the positions that contain the identifier.</p> <p>If <i>list1</i> is itself a list, the substring function is applied to all items in the list. The result is a list of substring values.</p>	<pre>substring(<i>list1</i>,<i>indexPosition1</i>, <i>indexPosition2</i>)</pre> <pre>substring([\$fdGroup1:fdStr1\$], 5)</pre> <pre>substring([\$fdGroup1:fdStr1\$], 5, 10)</pre>
split	Splits <i>string1</i> into a list by <i>delimiter</i> as the delimiter. The <i>delimiter</i> is regular expression.	split(<i>string1</i>,<i>delimiter</i>) Example: <pre>split('abc2def3ghi7','[0-9]')</pre> result is list of abc, def, ghi. Any digit from 0-9 is a delimiter.

Table 131. Examples of expressions for string operands and functions

Expression	Result	Note
'Control last updated on' + format (max ([\$Child:SoxControl/System Fields:Last Modification Date\$]))	Control last updated on October 29, 2020	Given that the object was last updated on October 29, 2020

Functions for lists and numerical values

Functions for lists and numerical values can be used in expressions.

For more information about lists and a video tutorial, see [“Working with lists” on page 349](#).

The following functions can be used on lists and numbers, including dates and currencies.

Table 132. Functions for lists and numbers

Function	Description	Syntax
append	Result is a list, where given items are appended at the end. Requires the list and the specified items to append.	append (listName, item1, item2,) Examples: append ([\$Child:object type/group:field name\$], 5, 10, 15) append([\$listOperation\$], 5, 10, 15) append([\$listOperation\$], 'test1', 'test2', 'test3') min (append ([\$objField1\$] , 0.0))
at	Result is the field value of the item at the specified index position. Count -1 returns the last item in the list.	at (listName, indexPosition) Examples: at ([\$Child:object type/group:field name\$], 5) at ([\$objField1\$], count ([\$objField1\$]) -1)
avg	Result is a numerical average. Requires one argument, which is an object field or list. Valid for numbers, currencies, and dates.	avg (listName) Examples: avg ([\$Child:object type/group:field name\$]) avg(5, 10, 15, 20) avg(list (5, 10, 15, 20)), builds the list and calculates the average
count	Result is the number of objects or items that are counted. Requires one argument, which is an object field or list. Can optionally use Append and Remove with count.	count (listName) Examples: count ([\$Child:object type/group:field name\$]) result is the number of child objects
list	Result is a list of items. Multiple arguments allowed.	list (listName, item1, item2,) Examples: list ('test1','test2','test3')
max	Result is the maximum value in a list of values. Valid for numbers, currencies, and dates.	max (listName) Examples: max ([\$Child:object type/group:field name\$])

Table 132. Functions for lists and numbers (continued)

Function	Description	Syntax
min	Result is the minimum value in a list of values. Valid for numbers, currencies, and dates.	min (listName) Examples: <code>min ([\$Child:object type/group:field name\$])</code> <code>min(5, 10, 15, 20)</code> <code>min(list(5, 10, 15, 20))</code>
remove	Result is a list, where specified items have been removed. Provide the list and the specified items to remove. If items occur multiple times in a list, all occurrences are removed.	remove (listName, item1, item2,) Examples: <code>remove(list('userA', 'userB', 'userC'), 'userB')</code>
round	Result is to round a value. Valid for numbers. If the argument is a list of values, the result is a list of rounded values.	round (number) Examples: <code>round ([\$Child:object type/group:field name\$])</code>
square	Result is the square value of a single number. Valid for numbers. If the argument is a list of values, the result is a list of squared values.	square (number) Examples: <code>square ([\$Child:object type/group:field name\$])</code>
sum	Result is a sum of a collection of values. Valid for numbers and currencies.	sum (listName) Examples: <code>sum ([\$Child:object type/group:field name\$])</code>

Table 133. Examples of expressions that use functions for lists

Expression	Result	Note
<code>count([\$Child:SOXBusEntity/OPSS-BusEnt:Entity Type\$])</code>	4	Given that there are 4 child objects
<code>at ([\$Child:SOXBusEntity/System Fields:Description\$], 5)</code>	Organizational Unit	Given that "Organizational Unit" is the description of the object in the 6th position.
<code>min(5, 10, 15, 20)</code>	5	
<code>list('test1', 'test2', 'test3')</code>	'test1', 'test2', 'test3'	Builds a list of items.
<code>count(list ('test1', 'test2'))</code>	2	Builds a list and counts the items in it.

Table 133. Examples of expressions that use functions for lists (continued)

Expression	Result	Note
<code>count (append([\$Child:object type/field\$] , 'test3'))</code>	Result is the number of child objects plus 1	Adds to a count.

Functions for dates

Date functions can be used in expressions.

Date functions can set an object field, be used in an if/else statement, or be used by other functions. There are also two system variables for dates, `[$TODAY$]` and `[$DaysFromNow/$]`.

The following functions can be used for dates:

Table 134. Functions for dates

Function	Description	Syntax
<code>add_days</code>	<p>Result is a date, the date given plus the number of days given. Requires two arguments.</p> <p>If <code>date</code> is a list of dates, the <code>add_days</code> function is applied to all items in the list. The result is a list of dates.</p>	<code>add_days(date, number)</code> Example: <code>add_days(2023-10-10, 2)</code> result is 2023-10-12.
<code>add_months</code>	<p>Result is a date, the date given plus the number of months given. Requires two arguments.</p> <p>If <code>date</code> is a list of dates, the <code>add_months</code> function is applied to all items in the list. The result is a list of dates.</p>	<code>add_months(date, number)</code> Example: <code>add_months(2023-10-10, 2)</code> result is 2023-12-10.
<code>add_year</code>	<p>Result is a date, the date given plus the number of years given. Requires two arguments.</p> <p>If <code>date</code> is a list of dates, the <code>add_year</code> function is applied to all items in the list. The result is a list of dates.</p>	<code>add_years(date, number)</code> Example: <code>add_years(2023-10-10, -2)</code> result is 2021-10-10.
<code>end_of_month</code>	<p>Result is a date that is the last day of the month, relative to the month in the date given. Requires one argument.</p> <p>If <code>date</code> is a list of dates, the <code>end_of_month</code> function is applied to all items in the list. The result is a list of month-end dates.</p>	<code>end_of_month(date)</code> Example: <code>end_of_month(2023-10-10)</code> result is 2023-10-31, if the date is in October <code>end_of_month([D1\$])</code> result is 2023-10-31 if the date is in October

Table 134. Functions for dates (continued)

Function	Description	Syntax
end_of_quarter	<p>Result is a date that is the last day of the quarter, relative to the date given. Requires one argument.</p> <p>If <i>date</i> is a list of dates, the <code>end_of_quarter</code> function is applied to all items in the list. The result is a list of quarter-end dates.</p>	end_of_quarter(<i>date</i>) Example: <code>end_of_quarter(2023-10-10)</code> result is 2023-12-31.
end_of_year	<p>Result is date that is the last day of the year, relative to the date given. Requires one argument.</p> <p>If <i>date</i> is a list of dates, the <code>end_of_year</code> function is applied to all items in the list. The result is a list of year-end dates.</p>	end_of_year(<i>date</i>) Example: <code>end_of_year(2023-10-10)</code> result is 2023-12-31.
today	Result is today's date. Requires no argument.	today() Example: <code>[\$D1\$] == (today)</code>
tomorrow	Result is tomorrow's date. Requires no argument.	tomorrow() Example: <code>[\$D1\$] == (tomorrow)</code>
yesterday	Result is yesterday's date. Requires no argument.	yesterday() Example: <code>[\$D1\$] == (yesterday)</code>

Regardless of how dates are displayed in your locale, the following expressions are valid:

Table 135. Examples of expressions that use dates

Expression	Result	Note
<code>[\$TODAY\$]</code>	2023-11-09	Given that today's date is November 9, 2023
<code>[\$TODAY\$]+10</code>	2023-11-19	Given that today's date is November 9, 2023
<code>2023-10-10 +30</code>	2023-11-09	
<code>format (2023-10-10 +30)</code>	November 9, 2023	
<code>end_of_month(today())</code>	2023-11-30	Given that today's date is in November 2023
<code>format (end_of_month(today()))</code>	November 30, 2023	Given that today's date is in November 2023
<code>format (end_of_quarter(today()))</code>	December 31, 2023	Given that today's date is in October, November, or December 2023

Functions for currency values

Functions for currency values can be used in expressions.

The following functions can be used for currencies:

Table 136. Functions for currencies		
Function	Description	Syntax
base_amount_of	<p>Result is base amount value from a currency function or currency object field.</p> <p>If the first argument is a list of currency values, the result is a list of base amounts.</p>	base_amount_of(currencyResult) Examples: <pre>base_amount_of(currency(1000.0 , 'EUR' , 1.1)) base_amount_of([\$field group:field name\$])</pre>
base_code_of	<p>Result is base currency code from a currency function or currency object field.</p> <p>If the first argument is a list of currency values, the result is a list of currency codes.</p>	base_code_of(currencyResult) Example: <pre>base_code_of([\$field group:field name\$])</pre>
currency	<p>Result is a representation of a currency amount, currency code, and exchange rate, where <i>exchangeRate</i> is optional. If omitted, the existing exchange rate for the currency is used.</p> <p>If the first argument is a list of integer or decimal values, the result is a list of currency values.</p>	currency(amount, currencyCode, exchangeRate) Examples: <pre>currency(1800000, 'JPY', 0.01) currency(3500.00, 'USD')</pre>
local_amount_of	<p>Result is local amount value from a currency function or object field.</p> <p>If the first argument is a list of currency values, the result is a list of local amounts.</p>	local_amount_of(currencyResult) Example: <pre>local_amount_of([\$field group:field name\$])</pre>
local_code_of	<p>Result is local currency code from a currency function or object field.</p> <p>If the first argument is a list of currency values, the result is a list of currency codes.</p>	local_code_of(currencyResult) Example: <pre>local_code_of([\$field group:field name\$])</pre>
ex_rate_of	<p>Result is exchange rate from a currency function or object field.</p>	ex_rate_of(currencyResult) Example: <pre>ex_rate_of([\$field group:field name\$])</pre>

Table 136. Functions for currencies (continued)

Function	Description	Syntax
system_ex_rate_of	Result is the system exchange rate, either current or for a specific date. Can have one or two arguments. Argument one is a currency code and two is a date. If currency code is given, result is the current system exchange rate for that currency. If two arguments are given, result is the system exchange rate for a currency code on a given date.	system_ex_rate_of(currencyCode, date) Example: <code>system_ex_rate_of('USD', 2022-12-01)</code> <code>system_ex_rate_of('USD')</code>

Examples:

Table 137. Examples of expressions that use currencies

Expression	Result	Note
<code>currency (1500, 'USD') + currency (150000.00, 'JPY', 0.01)</code>	local Currency =USD exchangeRate=1.0 baseAmount=3000.0 baseCurrency=USD localAmount=3000.0	
<code>format (currency (1500, 'USD') + currency (150000.00, 'JPY', 0.01))</code>	USD 3,000.00	

If/then/else/endif statements

An expression can contain an if/then/else/endif statement.

Table 138. If/then/endif statements in expressions

Function	Description	Syntax
if then elif else endif	<i>elif</i> is not required	if (condition) then action1 elif <...> else action N endif Example: <code>if ([\$fdGroup1:fdName1\$] == 'enum1') then 'Medium' else 'High' endif</code>

Table 138. If/then/endif statements in expressions (continued)

Function	Description	Syntax
Operands that can be used in conditions: == Equal != Not equal >Greater-than < Less-than >= Greater-than or equal <=Less-than or equal OR AND NOT AND NOT	Operands that can be used in conditions	Example: <pre>if ([\$abc\$] == 10 OR ([\$abc\$] == 20 AND NOT [\$def\$] == 15))</pre>
contains exists regex	Functions that can be used in conditions	Examples: <pre>exists([\$fdGroup1:fdName1\$]) contains([\$fdGroup1:string field\$], 'test') regex([\$fdGroup1:string field\$], '\d?abc.*')</pre>
in in_group matches_any in_hierarchy	Clauses that can be used in conditions	Examples: <pre>[\$fdGroup1:enum1\$] in ('aaa', 'bbb', 'ccc')</pre>

Basic example

```
if [$OPSS-Risk-Qual:Inherent Impact$] > 5 then "High Impact" else "Low Impact" endif
```

Result is High Impact, given that the value of [\$OPSS-Risk-Qual:Inherent Impact\$] is greater than 5

exists function

```
if exists([$System Fields:Name$]) then "Test BE Asia Pac" else "Not Found" endif
```

Result is: Test BE Asia Pac

contains function

```
if contains([$System Fields:Description$], 'test') then "Description has test" else "Not Found"  
endif
```

Result is: Description has test

regex function

```
if regex([$System Fields:Description$], '^(!test$.+)  
then "Result: ^ start of string , !test$).+ the string cannot be equal to test and .+ 1 or  
more characters"  
else "don't match"  
endif
```

The result is:

```
^ start of string , !test$).+ the string cannot be equal to test and  
.+ 1 or more characters
```

Syntax for nested if/then/else/endif statements

The following example illustrates the syntax for a nested if/then/else/endif statement. Note that a closing else block is always needed.

```
if ( A == 123 ) then  
    if ( B AND C ) then X1  
    elseif ( NOT B AND C ) then X2  
    else X3 endif  
elseif ( A == 456 ) then  
    if ( B AND C ) then X4  
    elseif ( NOT B AND NOT C ) then X5  
    else X6 endif  
else X7  
endif
```

Example: Inherent Exposure calculation on the SOXRisk object type

```
/**  
 * Risk Inherent Exposure  
 * The exposure value comes from the frequency multiplied by the severity.  
 * The frequency is derived from the Preference object based on the Likelihood.  
 * The severity is derived from the Preference object based on the Impact.  
 **/  
( if ([OPSS-Risk-Qual:Inherent Likelihood$] == '1') then [$Preference/OPSS-Pref:Freq1$]  
elif ([OPSS-Risk-Qual:Inherent Likelihood$] == '2') then [$Preference/OPSS-Pref:Freq2$]  
elif ([OPSS-Risk-Qual:Inherent Likelihood$] == '3') then [$Preference/OPSS-Pref:Freq3$]  
elif ([OPSS-Risk-Qual:Inherent Likelihood$] == '4') then [$Preference/OPSS-Pref:Freq4$]  
elif ([OPSS-Risk-Qual:Inherent Likelihood$] == '5') then [$Preference/OPSS-Pref:Freq5$]  
elif ([OPSS-Risk-Qual:Inherent Likelihood$] == '6') then [$Preference/OPSS-Pref:Freq6$]  
elif ([OPSS-Risk-Qual:Inherent Likelihood$] == '7') then [$Preference/OPSS-Pref:Freq7$]  
elif ([OPSS-Risk-Qual:Inherent Likelihood$] == '8') then [$Preference/OPSS-Pref:Freq8$]  
elif ([OPSS-Risk-Qual:Inherent Likelihood$] == '9') then [$Preference/OPSS-Pref:Freq9$]  
else [$Preference/OPSS-Pref:Freq10$] endif ) *  
( if ([OPSS-Risk-Qual:Inherent Impact$] == '1') then [$Preference/OPSS-Pref:Sev1$]  
elif ([OPSS-Risk-Qual:Inherent Impact$] == '2') then [$Preference/OPSS-Pref:Sev2$]  
elif ([OPSS-Risk-Qual:Inherent Impact$] == '3') then [$Preference/OPSS-Pref:Sev3$]  
elif ([OPSS-Risk-Qual:Inherent Impact$] == '4') then [$Preference/OPSS-Pref:Sev4$]  
elif ([OPSS-Risk-Qual:Inherent Impact$] == '5') then [$Preference/OPSS-Pref:Sev5$]  
elif ([OPSS-Risk-Qual:Inherent Impact$] == '6') then [$Preference/OPSS-Pref:Sev6$]  
elif ([OPSS-Risk-Qual:Inherent Impact$] == '7') then [$Preference/OPSS-Pref:Sev7$]  
elif ([OPSS-Risk-Qual:Inherent Impact$] == '8') then [$Preference/OPSS-Pref:Sev8$]  
elif ([OPSS-Risk-Qual:Inherent Impact$] == '9') then [$Preference/OPSS-Pref:Sev9$]  
else [$Preference/OPSS-Pref:Sev10$] endif )
```

Example: Inherent Rating calculation on the SOXRisk object type

```
/**  
 * Risk Inherent Rating  
 * The squared value of the likelihood and the impact is added up, then normalized from 0.0 to  
1.0.  
 * Based on the value, the Rating is set from "Low" to "Very High"  
**/  
if ( square( [$OPSS-Risk-Qual:Inherent Likelihood$] ) + square( [$OPSS-Risk-Qual:Inherent  
Impact$] ) )  
    >= ( square ( [$Setting/OpenPages/Solutions/ORM/Triggers/RCSA/XMAX$] ) +  
         square ( [$Setting/OpenPages/Solutions/ORM/Triggers/RCSA/YMAX$] ) ) * 0.75  
    then "Very High"  
    elif ( square( [$OPSS-Risk-Qual:Inherent Likelihood$] ) + square( [$OPSS-Risk-Qual:Inherent  
Impact$] ) )  
        >= ( square ( [$Setting/OpenPages/Solutions/ORM/Triggers/RCSA/XMAX$] ) +  
             square ( [$Setting/OpenPages/Solutions/ORM/Triggers/RCSA/YMAX$] ) ) * 0.5  
        then "High"  
    elif ( square( [$OPSS-Risk-Qual:Inherent Likelihood$] ) + square( [$OPSS-Risk-Qual:Inherent  
Impact$] ) )  
        >= ( square ( [$Setting/OpenPages/Solutions/ORM/Triggers/RCSA/XMAX$] ) +  
             square ( [$Setting/OpenPages/Solutions/ORM/Triggers/RCSA/YMAX$] ) ) * 0.25  
        then "Medium"  
    else "Low"  
endif
```

Example: KRI Indicator trend calculation

```
/**  
 * KRI Indicator trend  
 * Calculated by comparing recent two KRI Value Breach Status and set among Not Determined/  
Steady/Worse/Better  
**/  
// case1 : not enough KRI values  
if count( [$Child:KeyRiskIndicatorValue/OPSS-KRI-Shared:Breach Status/DescBy:OPSS-KRIVal:Value  
Date$] ) < 2 then "Not Determined"  
// case2 : one of the recent has "Not Determined"  
elif ( ( at( [$Child:KeyRiskIndicatorValue/OPSS-KRI-Shared:Breach Status/DescBy:OPSS-  
KRIVal:Value Date$], 0 ) == "Not Determined" ) OR  
      ( at( [$Child:KeyRiskIndicatorValue/OPSS-KRI-Shared:Breach Status/DescBy:OPSS-KRIVal:Value  
Date$], 1 ) == "Not Determined" ) ) then "Not Determined"  
// case 3 : two recent ones have the same breach status  
elif at( [$Child:KeyRiskIndicatorValue/OPSS-KRI-Shared:Breach Status/DescBy:OPSS-KRIVal:Value  
Date$], 0 ) ==  
      at ( [$Child:KeyRiskIndicatorValue/OPSS-KRI-Shared:Breach Status/DescBy:OPSS-KRIVal:Value  
Date$], 1 ) then "Steady"  
// case 4: The latest has "Red", which means prior one is "Yellow" or "Green"  
elif at( [$Child:KeyRiskIndicatorValue/OPSS-KRI-Shared:Breach Status/DescBy:OPSS-KRIVal:Value  
Date$], 0 ) == "Red" then "Worse"  
// case 5: The latest has "Green", which means prior one is "Yellow" or "Red"  
elif at( [$Child:KeyRiskIndicatorValue/OPSS-KRI-Shared:Breach Status/DescBy:OPSS-KRIVal:Value  
Date$], 0 ) == "Green" then "Better"  
// case 6 : The latest has "Yellow"  
elif at( [$Child:KeyRiskIndicatorValue/OPSS-KRI-Shared:Breach Status/DescBy:OPSS-KRIVal:Value  
Date$], 1 ) == "Red" then "Better"  
else "Worse" endif
```

Example: Audit Plan Actual T&E expenses

```
/**  
 * Audit Plan actual T&E aggregation  
**/  
if exists( [$Child:Timesheet/System Fields:Name$] ) then  
sum( [$Child:Timesheet/OPSS-Timesheet:Actual TE$] )  
else 0.0 endif
```

Example: Audit Plan Actual hours

```
/**  
 * Audit Plan actual hours aggregation  
**/  
if exists( [$Child:Timesheet/System Fields:Name$] ) then
```

```

sum( [$Child:Timesheet/OPSS-Timesheet:Monday$] ) +
sum( [$Child:Timesheet/OPSS-Timesheet:Tuesday$] ) +
sum( [$Child:Timesheet/OPSS-Timesheet:Wednesday$] ) +
sum( [$Child:Timesheet/OPSS-Timesheet:Thursday$] ) +
sum( [$Child:Timesheet/OPSS-Timesheet:Friday$] ) +
sum( [$Child:Timesheet/OPSS-Timesheet:Saturday$] ) +
sum( [$Child:Timesheet/OPSS-Timesheet:Sunday$] )
else 0.0 endif

```

Example: Audit Plan Helper

```

/***
 * URL for audit plan Helper
 ***/
[$APPLICATION_URL$] + "/Wizard/OPS_AuditAddModifyPlans.jsp?resourceId=" + [$System
Fields:Resource ID$]

<a style='color:#003F87' href='/Wizard/OPS_AuditAddModifyPlans.jsp?resourceId=' +
[$System Fields:Resource ID$] +
">" +
[$System Fields:Name$] +
</a>"

```

Running a calculation as an administrator

An administrator can run a calculation for multiple objects at once.

Before you begin

The calculation must be defined, enabled, and published. For more information, see [“Defining a calculation” on page 338](#).

Optionally, customize the content of email notifications. For more information, see [“Customizing email notifications for GRC Calculations” on page 366](#).

About this task

When an administrator runs a calculation, it runs for all objects that meet both the conditions that are defined in the calculation's applicability and conditions that are defined on the input fields.

You can run a single calculation at a time. It is not possible to start multiple calculations at once.

Procedure

1. Click  > **Solution Configuration > Calculations**.
2. Select the check box next to a single calculation and click  .
An estimated number of affected objects is displayed. The number reflects all objects that match the criteria that is defined in the calculation's applicability.
3. Click **Start Calculations** to continue.
4. Click Done.

Results

The calculation starts.

Track the progress and results by monitoring the following columns on the Calculation List:

- **In Queue**

Displays the total number of objects that are still to be processed.

- **Next In Queue**

Displays the next five objects in the queue to be processed. Click an object to open it in a Task View.

- **Error Count**

Displays the total number of objects that encountered an error.

Refresh the screen to display the latest information as the calculation progresses.

After the calculation finishes, an email is sent to the administrator who started the job.

What to do next

Review the email that you received as the administrator who started the calculation.

Check the results:

- Verify that the correct objects were updated.
- Verify that the calculation result is correct.

If the calculation failed for any objects, investigate the cause. For more information, see [“Testing and debugging a calculation” on page 365](#).

Testing and debugging a calculation

Verify the results of a calculation and resolve errors that are encountered.

There are several areas to review when testing and debugging a calculation:

- Accuracy

Does the calculation run without errors and update the correct fields?

Are the values in the updated fields correct?

- Interaction in a Task View

Is the user interaction in a Task View working as you expect?

- Applicability

Are the correct objects subject to the calculation?

- Conditions on the input field

Are the correct objects subject to the calculation?

- Errors

What error messages are issued? How can you use them to guide you to a resolution?

Errors for the current session display as notifications.

Note: Do not use the System Comment field (System Fields:Comment) in calculations.

Performance

How you design your calculation can affect the overall performance of OpenPages. For more information about designing calculations for better performance, see [“Understand how the design of the calculation can affect performance” on page 334](#).

Accuracy

Test the calculation by running it as an administrator.

If you run a calculation as an administrator, there are several ways you can watch for problems:

- Monitor the **In Queue**, **Next in Queue**, and **Error Count** columns in the Calculation List. Refresh the screen to display the latest information as the calculation progresses.
- Review the email that you received as the administrator who ran the calculation. The email lists all the objects that failed. Open those objects and review the error messages that are saved on the objects themselves.

Note: It is helpful when debugging a calculation to define a Grid View that contains the fields that a calculation should set. Run the calculation as an administrator and use the Grid View to quickly verify that the fields are set with the correct values. Continue to modify, run, and verify the results in the Grid View until the calculation is fully tested. Refresh the screen to display the latest information in the Grid View.

Interaction in a Creation View and a Task View

Test the calculation by creating an object with a Creation View. Then, test it in a Task View that users work with. When users are working on a Task View and add or change the value of a field that is an input field for a calculation, the calculation runs and the set fields are updated. If an error is encountered, an error message displays as the user is working. Verify the contents of the Task View and that the correct fields display. Be prepared to support users when they encounter errors and resolve the problems.

Applicability

Test that the correct objects are subject to the calculation. Review how the Applicability is defined on the calculation and test it thoroughly.

Conditions on input fields

Test that the correct objects are subject to the calculation. Review how conditions are defined on input fields in the calculation and test them thoroughly.

Error messages

When a calculation encounters a problem, an error message is saved on the object. The error message is cleared after the problem is resolved.

Error messages are assigned a unique ID so that you can match what happened in the UI with the stack trace in the aurora log file. For example, if the system issues an error, UJA0J1RX75PA-OP-11604, search for UJA0J1RX75PA in the log file. The descriptive text can also guide you to a solution.

If you get an error message `Insufficient information`, check that the calculation contains an `if exist/then/else` statement. This error can occur if the statement has no `else` statement, meaning that there is no default if none of the conditions are met.

Customizing email notifications for GRC Calculations

You can customize the content of the email notifications that are generated by GRC Calculations by defining application text that is specific to your organization.

Before you begin

Learn about starting calculations in bulk as an administrator. For information, see [“Running a calculation as an administrator” on page 364](#).

About this task

At the end of a bulk update process, an email notification is sent to the administrator who started the process.

You can use the default email template as-is or customize the text to meet your requirements. There is one email template for all calculations and all object types. You cannot create a new template.

If you operate in multiple locales, you can define email content in different languages. The template is designed for multiple formats, including tablets and phones.

If you customize the text, you define the content of the email notifications by using application text strings. The email subject content is plain text. The email body content is formatted in HTML. You can apply styles using embedded stylesheets.

You can also insert variables and fields in the email body content. The following variables are applicable to calculations:

- **[\${CALC_NAME\$}]** - calculation name
- **[\${OBJECT_COUNT\$}]** - number of objects processed
- **[\${SUCCESSFUL_CALCULATION_COUNT\$}]** - number of objects processed successfully
- **[\${DISPLAY_FAILURE\$}]** - includes failure information, if existent
- **[\${FAILED_CALCULATION_COUNT\$}]** - number of objects that failed
- **[\${FAILURES\$}]** - list of failures

Example:

```
<html>
  <head></head>
  <body style="font-family: ibm-plex-sans,HelveticaNeue,Helvetica,Arial,sans-serif; font-size: 14px;">
    <h1 style="font-size: 20px; font-weight: 300; padding: 22px 24px;">IBM <span style="font-weight: 600">OpenPages with Watson</span></h1>
    <hr style="margin: 0; border-bottom: 2px solid #0f62fe" />
    <div style="padding: 8px 24px 32px; background-color: #f3f3f3;">
      <h2 style="font-size: 14px; font-weight: 600; margin: 24px 0 8px;">Calculation name:</h2>
      <p style="margin: 0">[${CALC_NAME$}]</p>
      <h2 style="font-size: 14px; font-weight: 600; margin: 24px 0 8px;">Object type:</h2>
      <p style="margin: 0">[$System Fields:Object Type Label$]</p> </div>
      <div style="padding: 8px 24px 160px;">
        <h2 style="font-size: 14px; font-weight: 600; margin: 24px 0 8px;"> Number of objects evaluated:</h2>
        <p style="margin: 0">[${OBJECT_COUNT$}]</p>
        <h2 style="font-size: 14px; font-weight: 600; margin: 24px 0 8px;"> Number of calculations run successfully:</h2>
        <p style="margin: 0">[${SUCCESSFUL_CALCULATION_COUNT$}]</p>
        <div style="display:[${DISPLAY_FAILURE$}]">
          <h2 style="font-size: 14px; font-weight: 600; margin: 24px 0 8px;"> Number of calculations failed to run:</h2>
          <p style="margin: 0">[${FAILED_CALCULATION_COUNT$}]</p>
          <h2 style="font-size: 14px; font-weight: 600; margin: 24px 0 8px;"> Failed calculations (first 100 objects):</h2>
          <ul> [&${FAILURES$}] </ul> </div> </div>
          <hr style="margin: 0; border-bottom: 1px solid #767676" />
          <div style="padding: 32px 24px;">This email was automatically generated by
          [&$ApplicationText/product.name$].</div>
        </body>
      </html>
```

Procedure

1. Click  **System Configuration** > **Application Text**.
2. Click  to access the search filter.
3. Click **Email Templates**.
4. Open the **Email Templates** folder.
5. Use **Search** to further refine the list.
6. Select the application text you want to modify:
 - `com.calculation.email.template.bulk.run.subject` contains the text in the subject line.
 - `com.calculation.email.template.bulk.run.body` contains the text in the body of email.
 - `com.calculation.email.template.bulk.run.failure.part` contains a URL to the Task View that opens when an object in a list is clicked.
7. For each locale, enter the content that you want to appear in the email notification.

If it is displayed, click  to populate translated values to languages. For more information, see “[IBM Watson Language Translator](#)” on page 847.

8. Click **Done**.

Chapter 16. Configuring GRC Workflow

Using the GRC Workflow feature, you can design, configure, and administer workflow definitions and workflow instances for OpenPages.

Setting up GRC Workflow

You must configure workflows before users can access and use them.

Before you begin

Complete the following prerequisites:

- Learn about the GRC Workflow feature in OpenPages. For information, see “[GRC Workflow fundamentals](#)” on page 370.
- Learn about what you need to consider when you design a workflow. For information, see “[Designing a workflow](#)” on page 379.
- Learn about oversight users and the **Oversight Tasks** tab. For more information, see “[Types of users who interact with workflows](#)” on page 372 and “Using the Oversight Tasks tab” in the *IBM OpenPages with Watson User Guide*.
- Configure the UI before you configure the GRC Workflow feature with the exception of Task Views, which can be designed concurrently with GRC Workflow. For information, see “[Setting up the UI](#)” on page 229.
- Learn about GRC Calculations. For information, see Chapter 15, “Configuring GRC Calculations,” on page 327.
- Learn about the Scheduler. For information, see Chapter 17, “Scheduler,” on page 435.

About this task

During the configuration process, complete the following tasks to prepare for implementing workflows in OpenPages.

Procedure

1. Review your current implementation of triggers and configurable lifecycles and make changes accordingly.

When your organization adopts GRC Workflow, you can still use triggers and configurable lifecycles but you should make a plan to transition to workflow. You can design a landscape that uses all three features, but be aware of the limitations.

- You can use both triggers and workflows on the same object type but you must disable triggers that overlap with functionality in workflows. You can add custom actions to the workflows to accomplish what is currently achieved by triggers.
- You can use both configurable lifecycles and workflows for the same object type, but consider how they interact and where they conflict. For each object type, you can continue using configurable lifecycles or move what you currently accomplish with configurable lifecycles to workflows. If an object type has both a workflow and a configurable lifecycle, the workflow **Actions** button in Task Views takes priority over the lifecycle **Actions** button. Lifecycle fields that are used by configurable lifecycles are redundant in workflows. To disable lifecycles, remove the XML from the registry settings for lifecycles. For information, see *Configuring Triggers* in the *IBM OpenPages with Watson Trigger Developer Guide*.

2. Update the permissions for role templates for administrators who are configuring the workflows.
 - a) Click  > **Users and Security** > **Role Templates**.

b) Click a role template, and then go to the **Role Permissions** section.

c) Click **Edit**.

d) Select the **SOX > Administration > Workflow** permission.

Administrators with this permission enabled can define workflows with  > **Solution Configuration > Workflows**. They can also access and terminate workflow instances from **Manage Workflows**. For more information, see “[Managing workflow instances](#)” on page 431.

3. Click  > **System Configuration > Settings**.

4. Define the sender email address that is used for email notifications. It is defined in the **Applications > Common > Email** registry setting.

5. Define the maximum number of recipients for emails. It is defined in the **Platform > Workflow Implementations > OpenPages > Maximum Recipients Per Email** registry setting.

6. Define whether workflow information card content is updated automatically when changes are made to an object. It is defined in the **Platform > Calculation > Refresh Workflow Information Automatically** registry setting. If set to true, **Platform > Calculation > Enabled** must also be set to true. For more information, see “[How users interact with workflows](#)” on page 373.

7. Optional: Customize the content of the email notifications. Assignees and subscribers can receive email notifications for each action in a workflow. You can use the default email template or customize the text to meet your requirements. For information, see “[Customizing email notifications for GRC Workflow](#)” on page 432.

8. Review your implementation of Task Views or design them concurrently as you configure GRC Workflow. Learn about Task Views if you are not familiar with how to define and use them. For more information, see “[Task Views](#)” on page 251.

9. Define, test, and implement workflows. For information, see “[Defining a workflow](#)” on page 391.

What to do next

Complete the following post-requisites:

- Export workflow definitions from one environment to another, as needed. For information, see “[Exporting and importing workflow definitions](#)” on page 432.
- Monitor workflow instances. For information, see “[Managing workflow instances](#)” on page 431.
- Start workflow instances in bulk, as needed. For information, see “[Starting workflow instances in bulk](#)” on page 430.
- Report authors can include information from workflow instances in reports. For information, see “[Reporting on information in workflow instances](#)” on page 434.

GRCA Workflow fundamentals

OpenPages provides the framework that you use to define workflows and build task views that users access to start and interact with workflow instances.

Show me how

This video provides an overview of GRC Workflow and the Workflow Designer.

<https://youtu.be/ePnjAbRD0is>

Workflow definitions and workflow instances

The OpenPages GRC Workflow feature is based on workflow definitions and workflow instances.

You define workflows using the GRC Workflow Designer, which is a graphical editor. After you publish a workflow, it is available in OpenPages.

Workflow definitions

A workflow definition represents a business process and describes the tasks involved in the process. A workflow is defined for one object type. An object type can have multiple workflow definitions, for example, for Controls, you might have two workflows: Control Assessment and Control Change Request. The two workflows reflect two different business processes for Controls. Although an object type can have multiple workflow definitions, an object can be involved in only one workflow at a time. For example, if Control ABC is going through the Control Assessment workflow, you cannot start the Control Change Request workflow for it.

A workflow definition has the following characteristics:

- A workflow definition is static.

The actual execution of the workflow is described by the workflow instance, which holds the run-time information.

- A workflow definition is versioned.

Each time a workflow definition is published, a new version of that workflow definition is made available to users. The new version is used for workflow instances that are started after it is published. It does not affect workflow instances that are already running.

- A workflow definition can be disabled.

When a workflow definition is disabled, no new workflow instances based on that workflow definition can be started. Workflow instances that were already running when the workflow definition was disabled continue to run. Disabled workflow definitions can be re-enabled.

A workflow definition is made up of the following elements:

- Workflow properties define basic information about the workflow.

You can define how the workflow can be started (manually or automatically), a start schedule, the oversight user, the overall due date, applicability, and criticality normalization. For more information, see [“Defining workflow properties” on page 392](#).

- Stages represent tasks that are assigned to users.

There are three types of stages: start, end, and standard. For information, see [“Workflow stages” on page 397](#).

- Actions control the transitions between stages and the values on the **Actions** button.

An action contains comment settings, conditions, validations and operations, email notification settings, and a setting that controls whether the action runs in the background. For information, see [“Defining a workflow action” on page 407](#).

Workflow instances

As users work in OpenPages, they launch instances of workflow definitions. A workflow definition can have an unlimited number of workflow instances in progress at any given time.

Administrators can view and terminate active workflow instances. For more information, see [“Managing workflow instances” on page 431](#).

How workflows are started

The workflow properties defined how a workflow can start.

A workflow can be started in the following ways:

- Automatically when an object of the object type is created (if **Type** in the workflow properties is set to Auto Start).
- Manually when a user accesses the object and clicks an option on the **Actions** button if **Type** in the workflow properties is set to Manual Start.

- Automatically at set times if **Scheduled Start** in the workflow properties is defined. Workflows that are defined with a **Scheduled Start** automatically display as jobs in the Scheduler.
- By an administrator who clicks the **Start Job** option in the Scheduler (if the workflow is defined with a **Scheduled Start** in the workflow properties). For more information, see “[Managing jobs](#)” on page 435
- By an administrator who clicks the **Start Workflow** option on the Workflow List. For more information, see “[Starting workflow instances in bulk](#)” on page 430.

Note: If an object is locked, it must be unlocked before a workflow on the object can start.

After a workflow begins, other workflows start in the following ways:

- An action on a workflow can start another workflow for a related object.
- When a workflow ends, another workflow for the same object can start.

A workflow can have **Type** set to Auto Start or Manual Start and also be defined with a scheduled start. The type and scheduled start are independent of each other. If a workflow is set to Auto Start, a scheduled start can be used to restart a workflow that already ran and completed.

For all start methods, a workflow starts only if the **Applicability** conditions in the workflow properties are met.

You can use **Applicability** conditions to restrict when a workflow starts, for example, you can restrict who can start the workflow to a specific user or user group. Without these conditions, any user can start a workflow.

For a workflow that is defined to start on a schedule, you can, for example, use **Applicability** conditions to start a workflow only if a Review Date is equal to today's date. Another option is to start a workflow before a due date, relative to today's date. For example, if a workflow for Control objects starts 6 weeks before the next assessment is due, the team has enough time to complete the assessment. In this case, add an **Applicability** condition based on the due date field, set Expression to `[$TODAY$]`, set **Adjust Date By** to a specified value, and enter 42 in **Number of Days**.

For more information about **Type** and **Applicability**, see “[Defining workflow properties](#)” on page 392.

Types of users who interact with workflows

Three types of users interact with workflows: assignees, subscribers, and oversight users.

- Assignees

Assignees are users who own a task in a workflow. Assignees are defined per stage. There can be many assignees at a time for a task and different ones throughout a workflow process. Assignees view and find their assignments on the dashboard and My Tasks tab. If the assignee for a stage is a user group, the task is displayed on the dashboard or My Tasks tab for all users in the group. Any user in the group can pick up the task and complete it. Depending on how the workflow is configured, assignees can receive email notifications each time the stage changes and when a workflow ends. Assignees can also receive email reminders before, on, and after a stage due date.

- Subscribers

Subscribers are users who have an interest in one or more stages of a workflow. For example, the owner of the parent object in a workflow can be designated as a subscriber. Subscribers are frequently set to fields on the related object. They do not own tasks but they can complete tasks, if they choose to. They can act as a backup for the assignees. Subscribers are defined per stage. There can be many subscribers at a time for a task and different ones throughout a workflow process. Subscribers can view work that they are subscribed to on the Subscription Tasks tab. Depending on how the workflow is configured, subscribers can receive email notifications each time the stage changes and when a workflow ends. Subscribers can also receive email reminders before, on, and after a stage due date.

- Oversight users

An oversight user is someone who has overall responsibility for an area. Oversight users are defined per workflow. There can be none, one, or many oversight users for a workflow instance. Oversight

users are ordinarily at a management level, for example, Division Leads. In a situation where there are multiple divisions, each Division Lead can track workload and tasks for their teams. At any time during a workflow, they can add information to a task or complete it, if they choose to. Depending on how the workflow is configured, oversight users receive email notifications when a workflow ends. Otherwise, they do not receive email notifications. They access the Oversight Tasks tab, which summarizes tasks generated for workflows for their area. The Oversight Tasks tab summarizes tasks for assignees under one oversight user. Oversight users can drill down to the workload for specific individuals. Oversight users do not normally approve work or get assigned tasks unless a stage in the workflow also makes them an assignee or subscriber. In this case, they can access the dashboard or the My Tasks tab to view work that is assigned to them. They can access the Subscription Tasks tab to view what they are subscribed to.

See the *IBM OpenPages with Watson User Guide* for more information about the dashboard, My Tasks tab, Oversight Tasks tab, and Subscription Tasks tab.

How users interact with workflows

You can control aspects of the interaction between users and workflows. Your goal as a workflow designer is to create workflows that not only accurately model the business process but are also easy for users to finish and interact with.

As users work on their daily tasks, such as approving or rejecting tasks that are assigned to them, workflows work behind the scenes to orchestrate what happens next and who is involved. Users do not need a detailed understanding of the underlying workflow definitions or workflow instances. Messages and on-screen information guide them through the process to help them complete their tasks. They likely know only their part of the process and might not have a complete understanding of the full business process.

Starting a workflow

How a workflow can be started is defined in the workflow properties. For more information, see “[How workflows are started](#)” on page 371.

After a workflow starts, a workflow instance is created.

Stages become tasks

A stage in a workflow definition represents a task. Every time the stage changes, a new task is created.

Stages determine participants

A stage in a workflow definition determines the participants in the task, meaning the assignees and the subscribers.

Assignees access their tasks on the dashboard and My Tasks tab

Assignees access the dashboard and My Tasks tab to find their tasks. The dashboard can be configured but My Tasks tab requires no configuration.

Subscribers access their tasks on the Subscription Tasks tab

Subscribers access the Subscription Tasks tab to find tasks that they are subscribed to. The Subscription Tasks tab requires no configuration.

Assignees and subscribers access their tasks from emails

Assignees and subscribers can receive two types of emails:

- Email notifications
- Email reminders

Email notifications can be sent every time the stage changes and when a workflow ends. The recipient of the email can click a URL in the email to access the task. Emails notifications are defined on end stages and actions between stages. The content of the email notification can be used as-is or modified to meet your requirements. Email notifications are sent as single emails, which means that a user might receive multiple per day.

Email reminders can be sent before, on, and after the due date for a stage. The recipient of the email can click a URL in the email to access the task. Emails reminders are defined on standard stages. You can define who receives email reminders (assignees or subscribers). The content of the email notification cannot be modified. Email reminders are sent as a summary email, which means that a user receives one email per day regardless of the number of tasks that generated a reminder.

Email reminders are sent according to the following conditions:

- If the job runs every day, email reminders are sent according to the settings in the stage.
- If the job does not run on a day when the first reminder is to be sent, an attempt is made to send it when the job runs the next time.
- If the job does not run on the day when the "coming due" reminder is to be sent, an attempt is made to send it when the job runs the next time. When the reminder is sent also depends on when the last one was sent.
- If the job does not run on a day when a reminder is to be sent for a stage that is due, the reminder is not sent.
- If the job does not run on the day when the overdue reminder is to be sent, an attempt is made to send the reminder when the job runs the next time. When the reminder is sent also depends on when the last one was sent.

To avoid delayed reminders, schedule the job to run daily.

Oversight users access the Oversight Tasks tab

Oversight users access the Oversight Tasks tab to have a summary of the workload in their area of responsibility. Oversight users are defined in the overall workflow properties, not per stage. The Oversight Tasks tab lists all open tasks that belong to workflows that the oversight user is responsible for. The Oversight Tasks tab requires no configuration.

Users can access bulk workflow actions

If the bulk workflow actions feature in GRC Workflow is used, user can access their tasks by using the **Complete task with bulk workflow actions** window. If a user has open tasks, the window is displayed in the following locations:

- The My Tasks tab and dashboard panel.
- The Subscription Tasks tab and dashboard panel.
- The Oversight Task tab and dashboard panel.

Assignees interact with a Task View

A stage in a workflow definition determines the Task View that an assignee opens when they access the task. The Task View must contain the appropriate fields for that stage and what the user needs to accomplish. For example, if the assignee needs to set a date field at the stage, the field must be visible and editable. Two elements on a Task View help assignee understand what to do:

- User guidance

User guidance is customer-specific help text and field information that is displayed in the right panel. You define user guidance in the Task View. If a task is part of a workflow that has started, users can click **Select an action to validate** to check whether an action would pass validation before they complete the action. You can override the Task View's user guidance text with text that is specific to that stage. Use

this powerful feature to provide instructions and information that are specific to your organization and your business processes.

- Workflow information card

Workflow information is displayed in the right panel of any object that is in a workflow process. Called the *workflow information card*, this panel displays the stage that the object is at, the due date of the stage, and the current assignee. It is displayed regardless of who opens the object. You do not have to modify the task views to make it display.

Whether the workflow information card is automatically updated when an object is changed depends on the registry setting, **Platform > Calculation > Refresh Workflow Information Automatically**. If set to true, the content of the workflow information card is automatically updated and email notifications are sent if there is a change to assignees, subscribers, or oversight users. If set to false, the user must manually refresh the workflow information card.

Click the refresh button in the workflow information card if the workflow fields are not automatically updated with the latest changes. Fields that are displayed in the workflow information card are refreshed. If the dashboard or task tabs are open, information there is refreshed as well.

After a workflow is finished, the workflow information panel is no longer displayed.

Options on the Actions button drive the workflow

Assignees use the options on the **Actions** button to start workflows and complete their work and drive the workflow forward. You define the values that are displayed to users when you define actions between stages. Ensure that the names are short, active, and meaningful to the assignees.

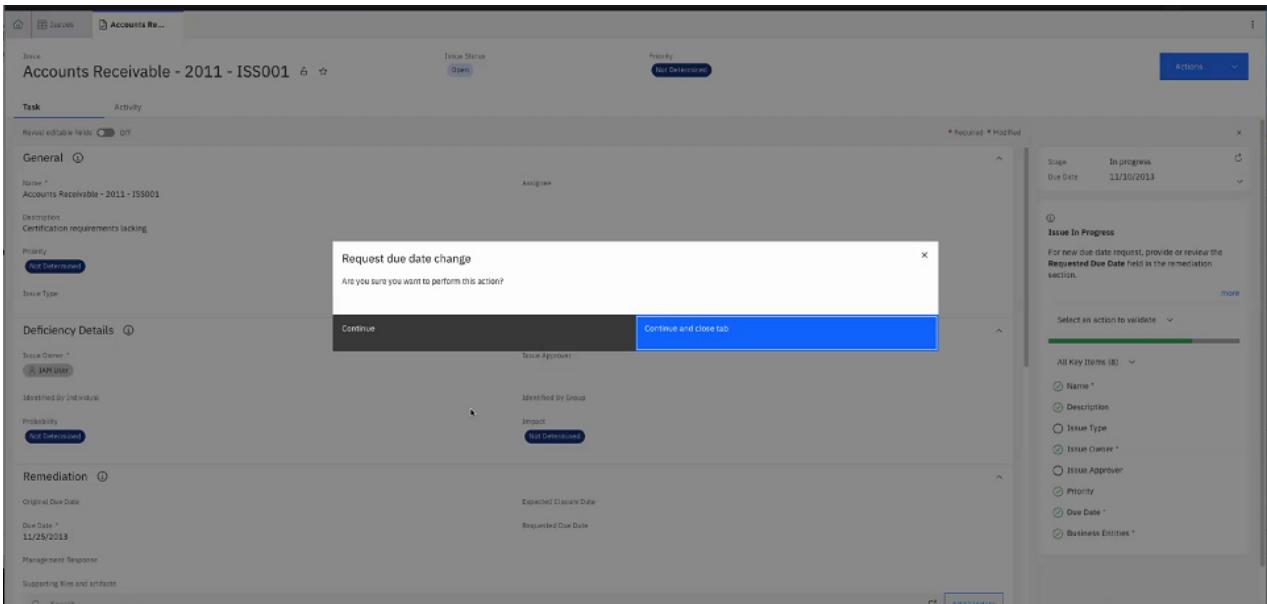
The order of the options on the **Actions** button is initially determined by creation order. If you rearrange the actions in Workflow Designer, the options on the **Actions** button are reordered based on the new arrangement. When the options are reordered, the first option on the list is the transition to the stage closest to the upper-left corner of the canvas.

If a user does not have permission to start the workflow or take the current action, no options are displayed on the **Actions** button. You can add an explanation to the user guidance to cover this situation.

Confirm the selected action

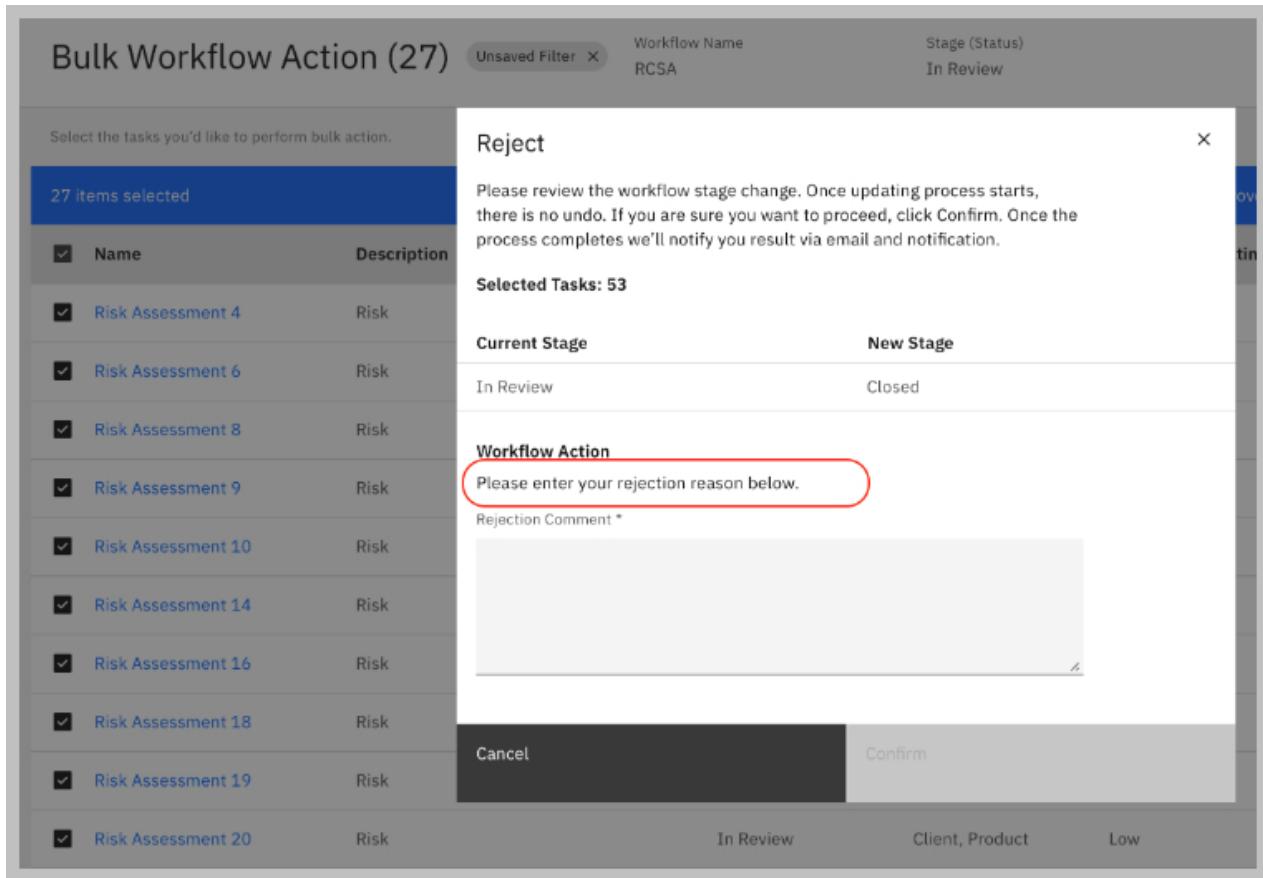
When a user chooses an action, a confirmation window is displayed. The access point determines the content of the confirmation window.

From a Task View, the confirmation window contains default content, as shown in this example:



The text on this confirmation can be customized by providing text on a workflow action in **Override workflow action text**. The text in **Override workflow action text** overrides the default text.

From a bulk workflow actions Grid View, the confirmation window contains more information, as shown in the following example:



Two texts of this confirmation window can be customized:

- You can add text at the position that is encircled in red by defining text on a workflow action in **Override workflow action text**.
- You can define text in the `app.taskView.confirmation.action.message` application text to control the text at the top.

Users can enter comments

Users can enter a comment (reason) that can be up to 4000 characters. Whether the comment window is displayed and whether it is required or optional is defined by the workflow action. For example, for an approval stage, you can define the workflow actions so that a user must provide a comment (reason) if the REJECT action is selected but a comment is optional if the APPROVE action is selected.

Focus on due dates

The due date for a task and the overall due date for a workflow are important to the participants in a workflow. For more information, see [“Interpreting and viewing due dates” on page 379](#).

System workflow fields

Information in a workflow instance is stored in system workflow fields.

You can include system workflow fields in Task Views, insert them in the email template, and include them in reports. When you define a workflow, you can reference system workflow fields in applicability,

conditions, validations, user assignments, and Filter By criteria where you can choose a field in the current object or in a related object. For example, you can reference a system workflow field in the current object or a related object in workflow Applicability conditions and in workflow action conditions and validations.

The following fields are system workflow fields:

- System Workflow Fields:Action Comment
- System Workflow Fields:Action Comment Date
- System Workflow Fields:Action Comment Owner (users or user groups)
- System Workflow Fields:Action Name (action label based on user's locale)
- System Workflow Fields:Action System Name (internal action name)
- System Workflow Fields:Assignees (users or user groups)
- System Workflow Fields:Last Action User (users)
- System Workflow Fields:Overseers (oversight users or user groups)
- System Workflow Fields:Performed Action (last performed action)
- System Workflow Fields:Stage Due Date
- System Workflow Fields:Stage Instance State (open, complete, or cancelled)
- System Workflow Fields:Stage Name (stage label based on user's locale)
- System Workflow Fields:Stage Start Date
- System Workflow Fields:Stage System Name (internal name)
- System Workflow Fields:Subscribers (users or user groups)
- System Workflow Fields:Workflow Criticality
- System Workflow Fields:Workflow Due Date
- System Workflow Fields:Workflow Name (workflow label based on user's locale)
- System Workflow Fields:Workflow Start Date
- System Workflow Fields:Workflow Start User (user) (for workflows that automatically start, this is the user who created the new object)
- System Workflow Fields:Workflow State (open, complete, cancelled, or executing)
- System Workflow Fields:Workflow Status (the label based on the user's locale of the Status field on actions)
- System Workflow Fields:Workflow Status System Name (the system name of the Status field on actions)
- System Workflow Fields:Workflow System Name (internal workflow name)

Using variables, functions, and fields

You can insert variables, object fields, system workflow fields, URLs, and application text in email templates and use them in the **expression** field. The **expression** field is part of **Applicability** in workflow properties and **Conditions, Validations, and Operations** in an action.

Variables

Table 139. Variables	
Enter	To insert/use
[\$APPLICATION_URL\$]	URL for OpenPages
[\$COGNOS_URL\$]	URL for IBM Cognos Analytics
[\$END_USER\$]	End user identifier

Table 139. Variables (continued)

Enter	To insert/use
[\$TODAY\$]	Today's date
[\$WORKFLOW_ACTION_USER\$]	User who completed the current action. It is used in the email template to show the user who sent an email notification.
[\$RULE_ASSIGNEES\$]	Users or groups assigned to the rule. It is used in automated workflows. The users or groups that are assigned to the rule are passed to the automated workflow.
[\$RULE_CRITICALITY\$]	Criticality of the rule. It is used in automated workflows. The Criticality of the rule is passed to the automated workflow. Valid values are: low, medium, high, or critical. Values are case-sensitive.

Functions

Table 140. Functions

Enter	To
trim	<p>Use the <code>trim</code> function to reduce the length of a string field. For example, apply in an Object Name field to ensure that the value does not exceed a set limit.</p> <p>Syntax:</p> <p><code>[\$field group:field name trim(length, replacementChar)\$]</code></p> <p>Function name is case-insensitive. Replacement character is optional.</p> <p>Examples:</p> <p>[\$RCM-TRRI-RegEv:Title trim(200,...)\$] Trims to first 200 characters of the field, replaces remaining additional characters with '!'.</p> <p>[\$RCM-TRRI-RegEv:Title trim(200,)\$] Trims to first 200 characters of the field.</p>

Fields, URLs, and application text

Table 141. Fields, URLs, and application text

To insert/use	Use the format
Object fields	<code>[\$field group:field name\$]</code>
System fields	<code>[\$System Fields:field name\$]</code>
A URL to an object task view	<code>[\$System Fields:Task View URL\$]</code>
Workflow field	<code>[\$System Workflow Fields:field name\$]</code> For example: <code>[\$System Workflow Fields:Action Label\$]</code>

Table 141. Fields, URLs, and application text (continued)

To insert/use	Use the format
Parent, child, preference field	[<i>\$Parent:object type/field group:field name\$</i>] [<i>\$Child:object type/field group:field name\$</i>] [<i>\$Preference/field group:field name\$</i>]
Application text content	[<i>\$ApplicationText/application text key\$</i>]
Object type name	[<i>\$System Fields:Object Type Label\$</i>]
Registry setting value	[<i>\$Setting/OpenPages/....\$</i>]
Day count from today to the stage due date	[<i>\$DaysFromNow/System Workflow Fields:Stage Due Date\$</i>]

Interpreting and viewing due dates

The different due dates involved in workflows assist users in completing their work on time.

Workflow due date and stage due dates

A workflow instance has an overall due date and each stage has a due date. The overall due date is displayed on the Oversight Tasks tab. The stage due dates are displayed on the workflow information card and on the users' dashboards. You can also add stage due dates and overall due dates to Task Views and Grid Views. A stage due date is based on the stage entry date (the date that the workflow instance enters the stage). If a workflow instance goes back to a stage, for example, it is rejected, the stage entry date is updated to today, and the due date is recalculated. All due dates are independent of each other. Due dates are calculated as calendar days, regardless of whether they are working or non-working days.

Object due date and assignee

Workflows have a due date field and an assignee field. However, an object can also have a due date field and an assignee field. The fields are unrelated. To avoid confusion, you might want to remove the object due date and object assignee fields from the views. You can also, optionally, copy the values from the workflow due date and assignee field to the object due date and assignee fields.

Designing a workflow

Designing a workflow involves knowing your business, understanding the workflow process, planning the workflow, planning the workflow participants, and designing the task views.

Know your business

Before you design a workflow, study the business process that the workflow is modeled on. Make sure that you understand every step in the process and what each person or department must accomplish. Ensure that you have a clear grasp of the business process before you get started. Make sure you also know who needs to approve your design and how the approval process works. You will want to share your design with the stakeholders and make revisions based on their input.

Plan the workflow process

After you understand the business process, plan the design of the workflow. You likely have several ways that you can approach it. Look at the pros and cons of each approach before you proceed.

- What is the driver for the workflow? Do you need multiple workflows or can you use one workflow and apply conditions on **Applicability** in the workflow properties? For example, is there a different workflow based on values in the object?
- How large is the workflow? You can break a large workflow into multiple smaller workflows. To link workflows together, you define actions that start workflows for related objects and end stages that start workflows for the same object. Add validation to make the workflows dependent on each other based on specific circumstances or results.

Take care that you do not create a situation where workflows go into an infinite loop and overload the system. For example, you can inadvertently create a cascading effect when one workflow starts 1000 workflows, each of those 1000 workflows starts another 1000 workflow, and so on. Safeguards are in place to avoid such a problem but they do not cover all possibilities.

- Does the workflow start automatically or manually?
- Does the workflow start on a set schedule?
- How many stages are there? Each stage creates a task.
- What needs to happen each time the stage changes? What validations need to occur at every stage change? What operations need to happen? Do fields need to be set or values calculated?
- What stages in the workflow do you want to allow users to complete as bulk workflow actions? For these stages, users can access tasks from the **Complete task with bulk workflow actions** window. It allows users to more quickly and efficiently work through the tasks they must complete.
- What are the options on the **Actions** button? What conditions must be met for an option to display? If options on the **Actions** button are displayed only to specific users, add text to the user guidance so that other users understand why no options are visible to them.
- Can a user provide a comment when they complete an action? If so, is the comment optional or required? For example, the rejection action on an approval stage can be defined to require the user to enter a comment. You can configure comments for all actions in a workflow except the initial action, which is from the start stage to the first standard stage. Plan how you want to use comment information and make it visible to other users. The workflow system fields for comment text, comment owner, and comment date can be included in task views and email notifications.
- Plan how often users receive email notifications in the workflow. Email notifications can be sent every time the stage changes and when a workflow ends. Plan the email notifications so that users are informed but not overloaded with emails.
- Plan when users receive email reminders. Emails reminders can be sent on a repeating schedule relative to a stage's due date. Plan the email reminders so that they effectively help users get their work done. Email reminders are sent as a summary email, which means that a user receives one email per day regardless of the number of tasks that generated a reminder.
- Are there points in the workflow when another workflow for a related object needs to start?
- Are there points in the workflow when child objects need to be created?
- Are there any points in the workflow when a calculation needs to be run?
- What are the cancellation or rejection paths in the workflow? At what point can a user cancel a task and what stage does the cancellation take them back to? What fields that were set by a field now need to be cleared? If an assignee must go back, how much work do they need to repeat? Plan paths in the workflow in both a forward and backward direction, as your business process requires.
- How many ways can the workflow end? You can define multiple end stages if a workflow can end in different scenarios. For example, you might have a workflow that can end in one of three ways.
 - End stage A: the workflow finishes successfully and fields 1, 2, and 3 on an object are set to the values A, B, and C.
 - End stage B: the workflow finishes successfully and fields 1, 5, and 6 on an object are set to values B, Z, and Y.
 - End stage C: the workflow is canceled and no actions are taken.
- Who needs to receive an email notification when a workflow ends? The oversight user and any other users you designate can receive an email notification when a workflow ends.

- Is the object finished when the workflow ends or does another workflow for the object need to start?
- What workflow information needs to be retained after the workflow finishes? After a workflow is finished, the workflow information on an object is no longer displayed. You need to save workflow information to objects to retain workflow information, for example, the completion date and the assignees.

Review the object structure

Understand the object structure. A workflow action that creates an object can create only a direct child object. But applicability in the workflow properties and conditions and validations on actions and the end stage can be based on field values on a related object that is a direct child, direct parent, ancestor, or descendant object.

Plan the workflow participants

After you plan the design of the workflow, map out who the workflow participants are.

- Who can start the workflow? You can restrict it by applying conditions on **Applicability** in the workflow properties.

The user who starts a workflow is saved in System Workflow Fields:Workflow Start User. Conditions where you can select **A field in the current object** or **A field in a related object** can be based on the value in this field.

- Who is the oversight user for the workflow? The oversight user is defined in the workflow properties.
- Who are the assignees for each stage? Assignees are defined by stage. The assignee gets a new task every time the stage changes. If the assignee for a stage is a user group, the task is displayed on the dashboard and My Tasks tab for all users in the group. Any user in the group can pick up the task and complete it.

The user who performed the most recently completed action is saved in System Workflow Fields:Last Action User. Conditions where you can select **A field in the current object** or **A field in a related object** can be based on the value in this field.

- Who are the participants for each stage? Participants are defined by stage.
- Who else has access to each stage of the workflow? Should users who are not workflow participants be allowed to see objects? You define access by setting the Access Type field on the stage properties.

Plan the Task Views

Workflows and task views work hand-in-hand. An existing Task View for an object type might be suitable for your workflow design or it might need slight changes. For example, if an assignee must set a date field during a task, ensure that the date field is in the Task View. If no existing Task View is suitable for the workflow, you can create a new one.

For information about what Task View is used by a workflow, see “[Defining a standard stage](#)” on page 397.

You can add workflow fields to a Task View. For information, see “[System workflow fields](#)” on page 376.

The **Actions** button that is defined in an action in a workflow takes precedence over the **Actions** button defined in a Task View.

Consider how to use Task View Overrides per stage when you plan fields, sections, user guidance, and key fields. You can use Task View Overrides to:

- Override whether a field is hidden or read only for a stage.
- Hide a section in a Task View or override the **Initially Collapsed** setting.
- Override the user guidance that is defined in a Task View with user guidance that is defined for a stage.
- Add the key fields that are defined in the Task View Overrides on a stage to the list of Key Fields in the user guidance panel, regardless of whether the user guidance is defined in the task view or the guidance text override.

An overall design decision that you might want to take is to use one Task View in many workflow stages. To do this, do not define user guidance in the Task View. Then, define highly specific user guidance in the Task View Overrides for each stage. Then you can more precisely control the user guidance that are displayed for each stage. And you have fewer Task Views to manage.

An overall design decision that you might want to take is to omit key fields from the user guidance in the Task Views. Instead, define key fields in the Task View Overrides on stages. You can then more precisely control the key fields that are displayed for each stage.

Plan the Grid Views for the bulk workflow actions

If you are using the bulk workflow actions feature, determine if existing Grid Views are adequate or whether you must define unique Grid Views. For more information, see “[Defining Grid Views for bulk workflow actions](#)” on page 259.

Review sample workflows

OpenPages provides sample workflows that you can as delivered or modify to meet your requirements. They can also be used as templates and learning tools for your own workflow. For more information, see the *IBM OpenPages with Watson Solutions Guide*.

Leverage the Preference objects

Review your organization's implementation of Preference objects. You can use Preference objects to hold entity-specific variable values that enable different behavior for different workflows.

- The assignee can be retrieved from the Preference object.
- The oversight user can be retrieved from the Preference object.
- Conditions on an action can be based on a Preference object.

When you use Preference objects, keep the following points in mind:

- Workflows do not use Preference Group objects. They use only Preference objects.
- The Preference object that is used is the one that is associated with the primary business entity parent (or ancestor) that is closest to the object where the workflow operation is occurring.
- The Preference objects of non-primary business entities are not used in workflows.
- When a primary parent business entity has multiple Preference objects, you can use all of the Preference objects that are associated with the primary parent business entity. Design your workflow to handle multiple Preference objects, for example by using applicability rules or conditions.

Note: Some of the sample workflows that are provided with OpenPages are not designed to manage multiple Preference objects for business entities. When you run one of these sample workflows, you might get an error such as Invalid field assignment or Multiple Preference objects on same entity causes workflow to fail: OP-08521.

For more information about Preference objects, see the *IBM OpenPages with Watson Solutions Guide*.

Plan the due dates

A workflow has an overall due date and each state has a due date. For more information, see “[Interpreting and viewing due dates](#)” on page 379.

Using the GRC Workflow Designer

The GRC Workflow Designer is a graphic interface that you use to define, publish, and manage workflows.

To open the GRC Workflow Designer, click  > **System Configuration** > **Workflows**. Whether the menu item is displayed depends on your access permissions.

Workflow list

The Workflow list shows workflows that are defined in the UI.

From the Workflow list, you can do the following tasks:

- Click **New Workflow** to create a new workflow. After you define the initial properties, the GRC Workflow Designer opens. For more information, see [“Defining a workflow” on page 391](#).
- Click a workflow. The GRC Workflow Designer opens. You can view or make changes to the workflow. Your work is automatically saved as you edit a workflow.
- Click a column header to change the sort order of the list.
- Select the check box next to a single workflow or multiple workflows to update numerous workflows. The bulk update options are:
 - **Delete** to delete the workflow.
 - **Enable** to set the **Enabled** property to **True**.
 - **Disable** to set the **Enabled** property to **False**.
 - **Start Workflows** to start a workflow instance for each object of the workflow's object type if all of the required conditions are met. For more information, see [“Starting workflow instances in bulk” on page 430](#).

Clear the check boxes to hide the bulk update options.

GRG Workflow Designer components

The GRC Workflow Designer has the following components:

- Canvas

The canvas is where you draw a workflow, create stages, and connect stages with actions.

- Toolbar

Icons on the toolbar allow you to create stages and control the view and the behavior of the canvas.

- Stage and action list panel

The stage and action list panel shows all stages and actions in the workflow. It can be displayed or hidden.

- Property panel

The content of the property panel changes depending on what you select on the canvas. It can be the workflow properties, a selected stage's properties, or a selected action's properties.

The following example shows the GRC Workflow Designer components with the stage and action list hidden.

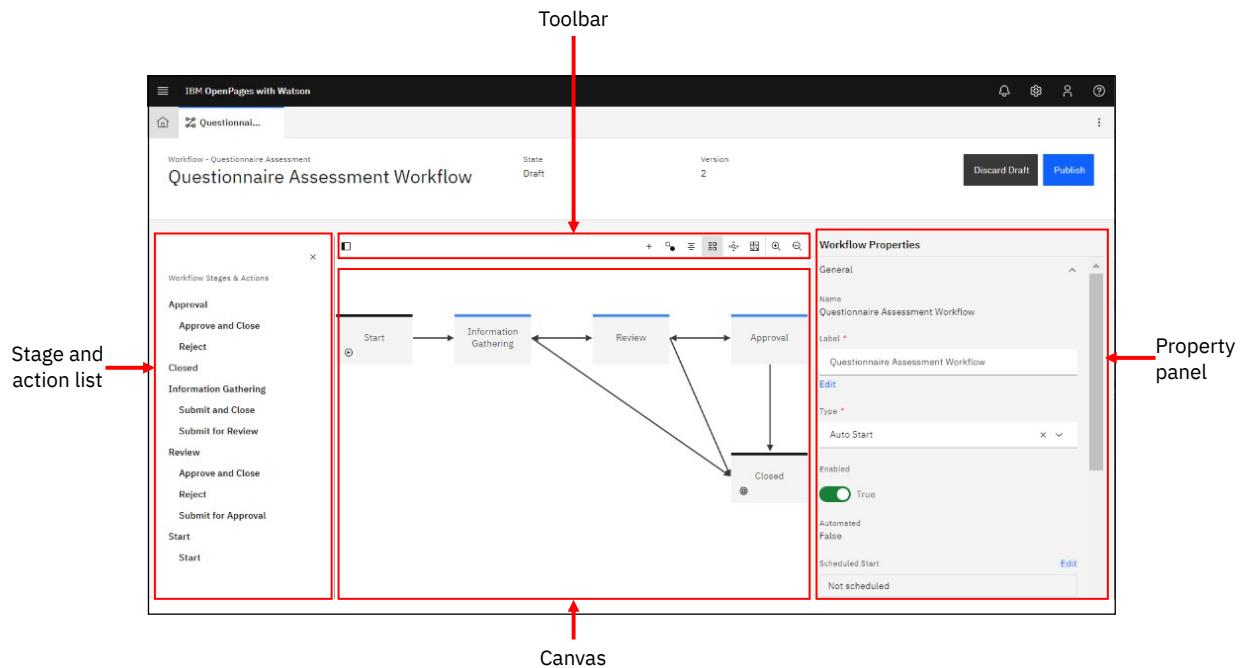


Figure 50. GRC Workflow Designer components

The GRC Workflow Designer toolbar contains the following icons:

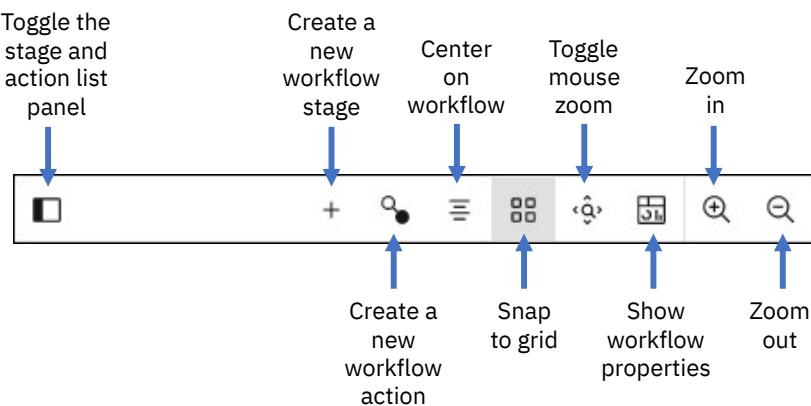


Figure 51. Toolbar icons

- **Toggle the stage and action list panel**
Opens and closes a panel that lists the stages and actions.
- **Create a new workflow stage**
Creates a new stage.
- **Create a new workflow action**

- Creates a new action.
- Center on workflow
 - Centers the workflow on the canvas.
- Snap to grid
 - Toggles snap to grid on or off. When snap to grid is on and you move an item on the canvas, the Workflow Designer uses an invisible grid to line up the items on the canvas along perfect horizontal and vertical lines.
- Toggle mouse zoom
 - Zooms out when scrolling down using the mouse wheel and zooms in when scrolling up using the mouse wheel.
- Show workflow properties
 - Displays the workflow properties in the property panel regardless of the item in focus on the canvas.
- Zoom in
 - Makes the items on the canvas appear larger and closer.
- Zoom out
 - Makes the items on the canvas appear smaller and farther away.

Using the keyboard in the GRC Workflow Designer

You can use your keyboard rather than your mouse to work with workflows in the GRC Workflow Designer. You can interact with workflow elements by using your keyboard to navigate the workflow canvas, toolbar, and property panel.

Key sequences

Use the following key sequences.

- Backspace on Windows or delete on macOS

Press Backspace on Windows or delete on macOS to display a dialog box that you can use to delete the item in focus on the canvas. The item in focus can be a stage or an action.

- Tab

In the canvas, press Tab to move the focus from the current stage to the next stage. When an action is in focus, press Tab to move the focus as though the stage it originates from was selected. For example, if you are working on the **Questionnaire Assessment Workflow** and the **Reject** action between the **Information Gathering** and **Review** stages is in focus, if you press Tab, the focus switches to the **Approval** stage.

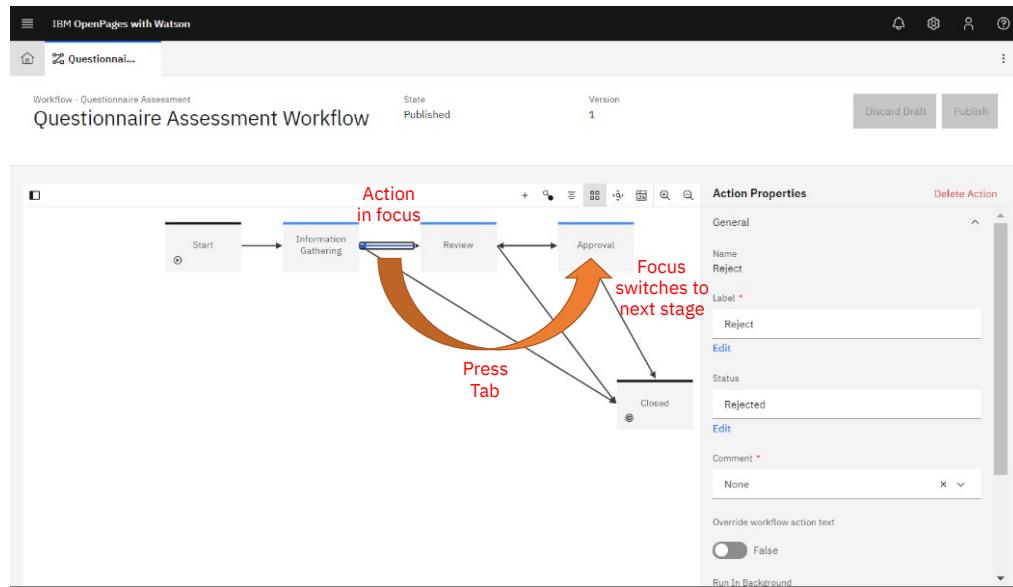


Figure 52. How pressing Tab works when an action is in focus

- Shift+Tab

In the canvas, pressing Shift+Tab moves the focus from the currently selected stage to the previous stage. When an action is in focus, press Shift+Tab to move the focus to stage it originates from. For example, if you are working on the **Questionnaire Assessment Workflow** and the **Reject** action between the **Information Gathering** and **Review** stages is in focus, if you press Shift+Tab, the focus switches to the **Review** stage.

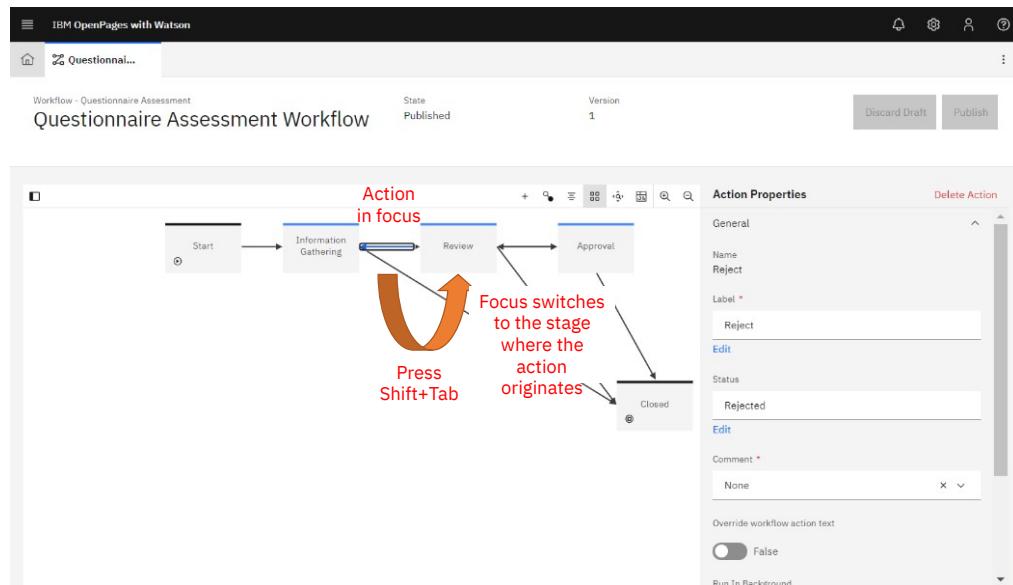


Figure 53. How pressing Shift+Tab works when an action is in focus

- Enter on Windows or return on macOS

When you first open the GRC Workflow Designer, the general property panel for the workflow is displayed. If you change the focus in the canvas to another stage or action and press Enter on Windows or return on macOS, the property panel displays the properties for the stage or action in focus and the cursor moves to the end of the text in the **Label** text box of the property panel. For example, if you open the **Questionnaire Assessment Workflow** and you tab to the **Information Gathering** stage in the canvas, the property panel still shows the general properties for the workflow. If you press Enter on Windows or return on macOS, the property panel switches to the **Information Gathering** stage properties and the cursor moves to the end of the text **Information Gathering** in the **Label** text box of the property panel.

The **Return focus** and **Delete Stage** links appears in the banner of the property panel.

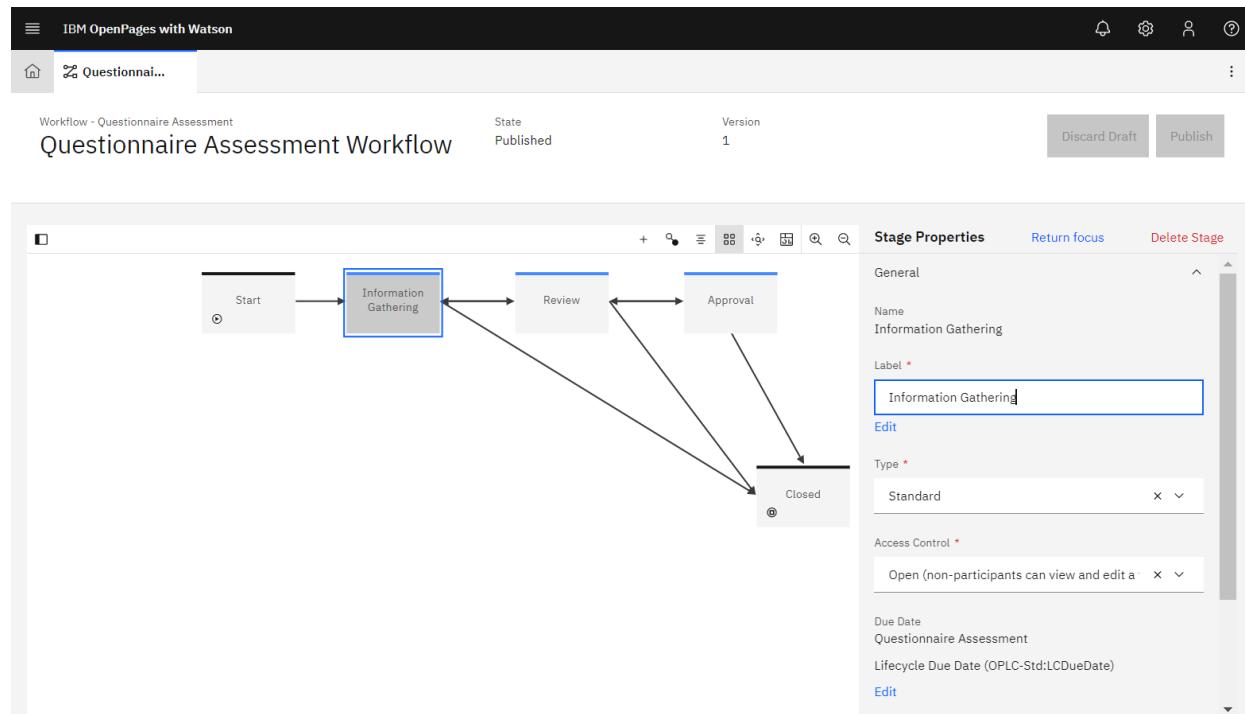


Figure 54. How the property panel appears after pressing Enter when a stage is in focus

- right arrow key

Use the right arrow key to move among the actions that are connected to the stage in focus in a clockwise order starting on the right side.

If you close the workflow tab and reopen it, pressing the right arrow moves to the next action clockwise from the action selected when the workflow tab was last open.

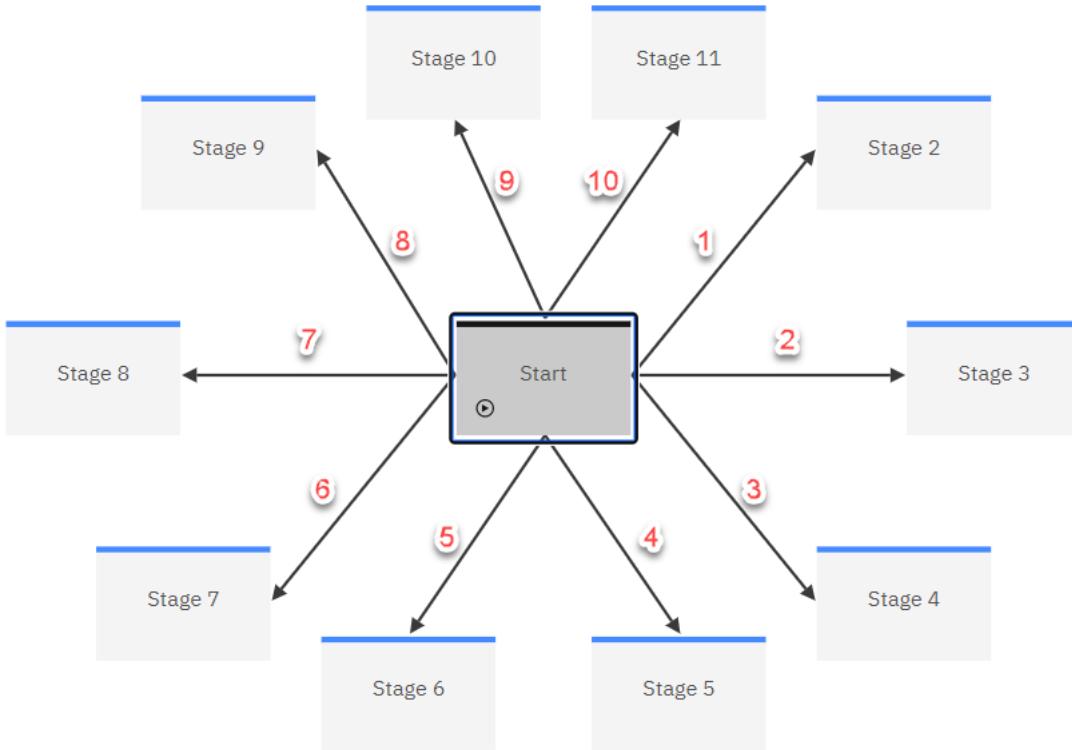


Figure 55. Workflow Designer canvas showing the order of actions selected when the Start stage is in focus and the right arrow is pressed

- left arrow key

Use the left arrow key to move among the actions that are connected to the stage in focus in a counterclockwise order starting on the left side.

If you close the workflow tab and reopen it, pressing the left arrow moves to the next action counterclockwise from the action selected when the workflow tab was last open.

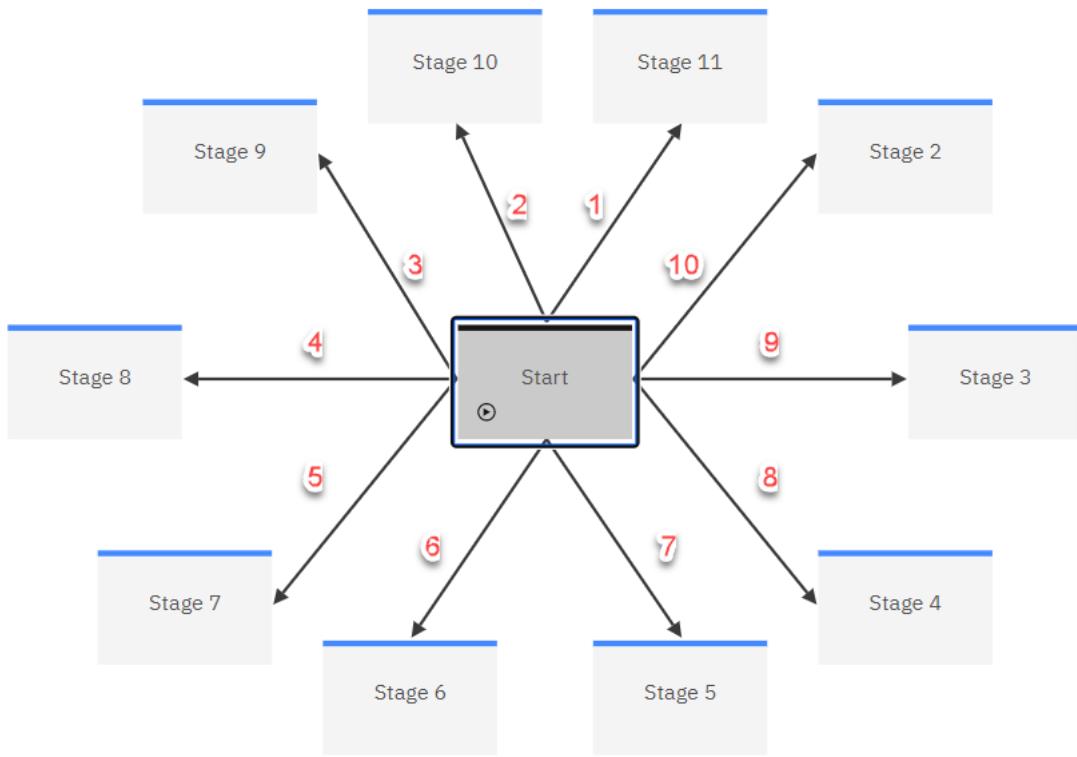


Figure 56. Workflow Designer canvas showing the order of actions selected when the Start stage is in focus and the left arrow is pressed

- ⌘+arrow keys (macOS) or Ctrl+arrow keys (Windows)

Use this key sequence to move the stage in focus on the canvas. The left arrow key moves the stage to the left and the right arrow key moves the stage to the right.

- ⌘+option+n (macOS) or Ctrl+Alt+n (Windows)

Use this key sequence to open a dialog box where you can create an action on the stage in focus.

Hyperlinks

Press Tab to move to the following hyperlinks in the banner of the property panel.

- **Return focus**

To return focus to the stage or action in the canvas from the property panel, press Shift+Tab to navigate to the **Return focus** link and press Enter on Windows or return on macOS.

- **Delete Stage**

When a stage on the canvas is in focus, the **Delete Stage** hyperlink is displayed in the banner of the property panel. Press Enter on Windows or return on macOS when you are on the **Delete Stage** hyperlink to delete the stage in focus.

- **Delete Action**

When an action on the canvas is in focus, the **Delete Action** hyperlink is displayed in the banner of the property panel. Press Enter on Windows or return on macOS when you are on the **Delete Action** hyperlink to delete the action in focus.

Toolbar icons

Press Tab to move to the following icons in the banner of the canvas.

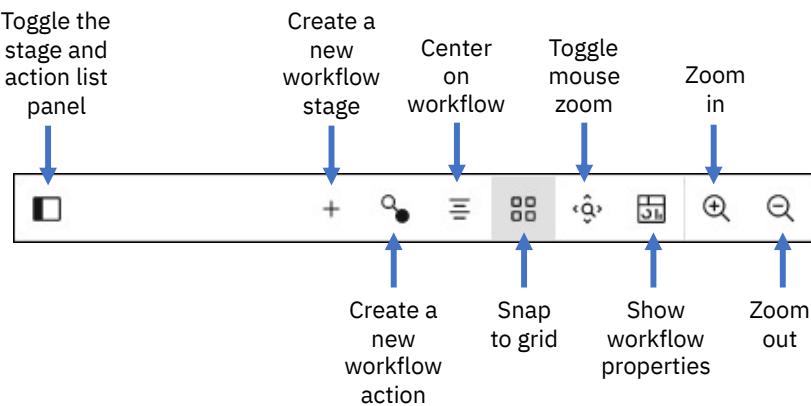


Figure 57. Toolbar icons

- **Toggle the stage and action list panel**

Press Enter on Windows or return on macOS to open a panel that lists the stages and actions. To close the panel, Press Enter on Windows or return on macOS again.

- **Create a new workflow stage**

Press Enter on Windows or return on macOS to open a dialog box where you can create a new stage.

- **Create a new workflow action**

Press Enter on Windows or return on macOS to open a dialog box where you can create a new action.

- **Center on workflow**

Press Enter on Windows or return on macOS to center the workflow on the canvas.

- **Snap to grid**

Press Enter on Windows or return on macOS to toggle snap to grid on or off. When snap to grid is on and you move an item on the canvas, the Workflow Designer uses an invisible grid to line up the items on the canvas along perfect horizontal and vertical lines.

- **Toggle mouse zoom**

Press Enter on Windows or return on macOS to zoom out when scrolling down using the mouse wheel and zoom in when scrolling up using the mouse wheel.

- **Show workflow properties**

Press Enter on Windows or return on macOS to display the workflow properties in the property panel regardless of the item in focus on the canvas.

- **Zoom in**

Press Enter on Windows or return on macOS to make the items on the canvas appear larger and closer.

- **Zoom out**

Press Enter on Windows or return on macOS to make the items on the canvas appear smaller and farther away.

Defining a workflow

A workflow definition contains basic information, stages, and actions.

Before you begin

Complete the following prerequisites:

- Complete the steps listed in “[Setting up GRC Workflow](#)” on page 369.
- Learn about how to use the GRC Workflow Designer. For more information, see “[Using the GRC Workflow Designer](#)” on page 382.
- Learn about the Scheduler. For more information, see “[Managing jobs](#)” on page 435.
- Design the workflow. For more information, see “[Designing a workflow](#)” on page 379.
- Review the Task View that the workflow uses and make sure it has the content you need. For more information, see “[Task Views](#)” on page 251.

Procedure

1. Click  > **Solution Configuration** > **Workflows**.

2. Click **New Workflow**.

3. Complete the following workflow properties and click **Create**.

a) Leave **Enabled** selected. It can be changed later.

b) Enter an internal **Name** for the workflow. It cannot be changed later.

Allowed characters are A-Z, a-z, 0-9, underscore, hyphen, and spaces. Special characters are not allowed.

c) Select an **Object Type**. It cannot be changed later.

d) Select Auto Start or Manual in **Type**. It can be changed later.

For more information, see “[Defining workflow properties](#)” on page 392.

The workflow canvas opens with one default stage, the start stage. The word *Draft* and the version number, v1, are displayed next to the workflow name. You can begin defining the workflow.

4. Leave the start stage. A workflow can have only one start stage. Click **Edit** next to **Label** to add labels to the start stage.

5. Define the standard stages.

For information, see “[Defining a standard stage](#)” on page 397

6. Define the end stages.

For information, see “[Defining an end stage](#)” on page 402.

7. Connect the stages with actions. For more information, see “[Defining a workflow action](#)” on page 407.

Note: You can define a stage and not connect it with an action to another stage. It is not considered an error in the workflow definition. However, the stage is not processed by the workflow. You can use this feature, for example, to define draft stages and workflow branches that you want to save for future use.

8. Optional: If you want to discard changes you made to a workflow, click **Discard Draft**. All changes since the last published version are discarded.

9. When you are ready to test the workflow, click **Publish**.

The v1 version of the workflow becomes the first published version of the workflow.

If the workflow is defined with a scheduled start, a job for the workflow is automatically added to the Scheduler as a job. The job name is a concatenated value of the workflow name, the object type, and - Scheduled Start. A schedule on a workflow cannot be changed in the Scheduler. But you can

enable, disable, and start the job. On the linked detail page, you can change the description and view the schedule.

10. Test the workflow. If you need to make changes to the workflow, open it again in the GRC Workflow Designer. Since you are now opening a published workflow, the word *Published* appears, the version number is displayed next to the workflow name and the **Publish** button is grayed out. When you make a change to the workflow, *Published* changes to *Draft*, the version number is incremented by 1, and the **Publish** button becomes active.

To discard changes you make to a workflow, click **Discard Draft**. All changes since the last published version are discarded.

Note: Each time you change the workflow, you need to publish it and re-test it.

It might be helpful to turn on trace logging for the workflow during testing and error resolution. For information, see “[Enabling trace logging](#)” on page 698.

Each time a workflow definition is published, a new version of that workflow definition is made available to users. The new version is used for workflow instances that are started after it is published. It does not affect workflow instances that are already running.

Results

You can work on the workflow as a team. When you have a workflow open in the GRC Workflow Designer, the URL contains the workflow's internal name. If you are working on the workflow with colleagues, you can send them the URL to share your progress. Although you can collaborate with colleagues, only one user should work on a workflow in the GRC Workflow Designer at a time.

Defining workflow properties

A workflow has a set of properties that control its overall functionality.

Before you begin

Define basic information (name and object type) for the workflow. For more information, see “[Defining a workflow](#)” on page 391.

Procedure

1. Click  > **Solution Configuration** > **Workflows**.
2. Click the workflow that you want to edit.
The GRC Workflow Designer opens.
3. Click anywhere in the empty area of the canvas.
The Workflow Properties panel opens. All of the properties can be edited except **Name** and **Object Type**, which is hidden.
4. Enter a **Label** for the workflow.
Allowed characters are A-Z, a-z, 0-9, underscore, hyphen, and spaces. Special characters are not allowed.
If the workflow is used in multiple locales, enter a workflow label for each language.

If it is displayed, click  to populate translated values to languages. For more information, see “[IBM Watson Language Translator](#)” on page 847.

Workflow labels are displayed on the dashboard, My Tasks tab, Subscription Tasks tab, and Oversight Tasks tab.

5. Define how the workflow is launched in **Type**:
 - Auto Start

The workflow is launched automatically when an object of the object type is created, either by creating new or creating a copy of another object. During a copy, a workflow starts for the main object that is created but not for sub-objects that are created.

- Manual Start

The workflow is launched when a user accesses the object and clicks an option on the **Actions** button.

6. Set **Enabled** to true or false. Only enabled workflows can be started.
7. Click **Edit** next to **Scheduled Start** to set up a repeatable schedule. Otherwise, leave **Schedule** set to Not scheduled.

- a) Enter a **Name**.

The **Name** displays in the Scheduler as the **Schedule Name**. Allowed characters are A-Z, a-z, 0-9, underscore, hyphen, and spaces. Special characters are not allowed.

- b) Enter a **Description** (optional).

- c) Select a schedule type in **Define Schedule**:

- Recurring
- Specified Date/Time
- Cron Expression

- d) If you chose Recurring:

- Select a value in **Repeat** (Daily, Weekly, Monthly, Quarterly) and add details such as day, month, or quarter.
- Enter a **Time of Day**.
- Select an **End Date** (optional).

- e) If you chose Specified Date/Time:

- Select a **Date**.
- Enter a **Time of Day**.

- f) If you chose Cron Expression:

- Enter a **Cron Expression**.
- Select an **End Date** (optional).

Advanced users can choose a cron expression if a Recurring or Specified Date/Time schedule does not meet your needs. Use the syntax for cron expressions, not crontab expressions.

- g) Click **Done**.

8. Set **Execute As System** to **False** to execute the action as the logged in user. Set **Execute As System** to **True** to execute the action as the OPSSystem user. The action can then perform operations that the logged in user cannot. The history on the **Activity** tab shows OPSSystem as the user who performed the action.

When you set **Execute As System** to **True**, all set field operations where **Target Objects** is set to **Self** are also executed as the OPSSystem user.

9. Set **Automated** to true or false. Automated workflows do not have standard stages, only one start and one or more end stages. An automated workflow progresses from one stage to another automatically, without user interaction. Automated workflows are used in IBM OpenPages Regulatory Compliance Management. For more information, see “[Processing regulatory events by using rules](#)” on page 911.

10. Designate the **Oversight** users. These are users in the organization who have oversight responsibility for activity that is generated by the workflow. Their work is summarized on the Oversight Tasks tab. You can select only actor fields. Do not select a system workflow field such as *System Workflow Fields:Overseers*. You can assign multiple oversight users to a workflow. They can be from multiple sources, for example, a specific user, a field on the current object, and a field on a related object.

- a) Click **Add Oversight**. In **Assign To** choose what value to set the oversight user to:

- **Users or Groups**
- **A field in the current object**
- **A field in a related object**
- **A field in a preference object**

The panel changes depending on your selection.

- Complete the panel.
- Click **Done**.

11. Define how the **Overall Due Date** for the workflow is determined.

In **Assign To** choose what value to set the overall due date to:

- **Workflow Start Date** (the date the workflow instance starts)
- **A specified value**
- **A field in a related object**
 - Select Direct Child, Direct Parent, Ancestor, or Descendant in **Relationship Type**.
 - Select an object type in **Related Object Type**.
 - Select a path in **Relationship Paths** (displays only if **Relationship Type** is Ancestor or Descendant).
 - Select a field in **Related Object Field**.
 - Add **Filter By** conditions (optional).
 - Set **Primary Parent Only** (displays only if **Relationship Type** is Direct Parent or Ancestor) (optional).

You can optionally add **Filter By** conditions and set **Advanced Logic**.

- **A field in the Preference object**

You can optionally add **Filter By** conditions.

In **Adjust Date By** you can optionally define an offset for the date you chose in **Assign To**. The offset can be:

- **A specified value** and enter **Number of Days**.
- **A field in the current object**
- **A field in a related object**
 - Select Direct Child, Direct Parent, Ancestor, or Descendant in **Relationship Type**.
 - Select an object type in **Related Object Type**.
 - Select a path in **Relationship Paths** (displays only if **Relationship Type** is Ancestor or Descendant).
 - Select a field in **Related Object Field**.
 - Add **Filter By** conditions (optional).
 - Set **Primary Parent Only** (displays only if **Relationship Type** is Direct Parent or Ancestor) (optional).

You can optionally add **Filter By** conditions and set **Advanced Logic**.

- **A field in the Preference object**

You can optionally add **Filter By** conditions.

12. In **Applicability** you define the conditions under which the workflow starts. Expand **Applicability** and click **New Condition**. The **Applicability** panel opens.

- Leave blank if only one workflow is defined for the object type and if any user can start the workflow without restriction.

- Add conditions if multiple workflows are defined for the object type. The conditions in **Applicability** determine which workflow is started for a specific object. **Applicability** is especially important if **Type** is set to *Auto start*.
- Add a condition if you want to restrict who can start the workflow. The condition determines which users or user groups are allowed to start the workflow. Without this condition, any user can start the workflow.
- Add a date condition to additionally restrict a workflow that starts on a schedule (optional). For example, define a condition that Review Date must be equal to today. Like all workflows, a workflow that is defined to start on a schedule must meet the **Applicability** conditions to start.
- For each condition, you build a comparison statement with two fields and an operator.
- If you define multiple conditions, all conditions must be met for the workflow to start.

To override this rule, define **Advanced Logic** to combine the conditions in a specific way.

- a) In **Compare**, you define the first field in the comparison statement. You can choose:

- **A field in the current object**

Select an **Object Field**.

- **A field in a related object**

- Select Direct Child, Direct Parent, Ancestor, or Descendant in **Relationship Type**.
- Select an object type in **Related Object Type**.
- Select a field in **Related Object Field**.
- Select a path in **Relationship Paths** (displays only if **Relationship Type** is Ancestor or Descendant).
- Add **Filter By** conditions (optional).
- Set **Primary Parent Only** (displays only if **Relationship Type** is Direct Parent or Ancestor) (optional).

- **A field in a Preference object**

Select a **Preference Object Field**. You can add **Filter By** conditions.

- **End User**

An **End User** condition checks whether the signed on end user is a specified user and whether the user is in a specified user group. The second field in the comparison statement is a specified value, an expression, or an actor field on an object.

- b) In **Using**, choose an **Operator**. The list of operators depends on the field type of the field you chose in **Compare**.

- c) In **To**, you define the second field in the comparison statement. You can choose:

- **A specified value**

The value that you can provide depends on the field type of the field you chose in **Compare**. The comparison is case sensitive, so ensure that you specify the correct case for the value.

- **An expression**

Enter a single field or variable from the list in “[Using variables, functions, and fields](#)” on page 377. All of the variables and fields listed there can be used in an expression. The field or variable must be in the given format. It can, however, be part of a longer string, for example, a file name like Evidence_[\$Parent:SOXRisk/System Fields:Name\$].pdf if you want to validate that the parent object has a specific PDF attachment.

- **A field in the current object**

Select an **Object Field**.

- **A field in a related object**

- Select **Direct Child, Direct Parent, Ancestor, or Descendant** in **Relationship Type**.

- Select an object type in **Related Object Type**.
- Select a field in **Related Object Field**.
- Select a path in **Relationship Paths** (displays only if **Relationship Type** is Ancestor or Descendant).
- Add **Filter By** conditions (optional).
- Set **Primary Parent Only** (displays only if **Relationship Type** is Direct Parent or Ancestor) (optional).

- **A field in a Preference object**

Select a **Preference Object Field**. You can add **Filter By** conditions.

- d) If you chose a date field in **Compare**, you can define an offset in **Adjust Date By**.

- **A specified value** and enter **Number of Days**.
- **A field in the current object**
- **A field in a related object**
 - Select Direct Child, Direct Parent, Ancestor, or Descendant in **Relationship Type**.
 - Select an object type in **Related Object Type**.
 - Select a field in **Related Object Field**.
 - Select a path in **Relationship Paths** (displays only if **Relationship Type** is Ancestor or Descendant).
 - Add **Filter By** conditions (optional).
 - Set **Primary Parent Only** (displays only if **Relationship Type** is Direct Parent or Ancestor) (optional).

- **A field in the Preference object**

You can add **Filter By** conditions.

- e) Click **Done**.

The condition is saved and assigned a number. Conditions are numbered consecutively in the order they are defined.

- f) Optional: Add more conditions.

- g) Optional: Set **Advanced Logic** to true to override the default rule that all conditions must be met. Write a statement in **Logic**. Use the condition numbers together with the operators and, or, not, and parentheses.

The order of operations is: () then NOT then AND then OR.

For example:

- 1 or 2 or 3
- 1 and (2 or 3)
- 1 not (2 or 3)

13. Define the **Criticality**. Select a single value enumerated field that contains the criticality of the object type for this workflow, and map its values to standard values (low, medium, high, and critical).

Each object type in OpenPages can use a different field for criticality. When you map the object fields to standard values, you normalize the values across object types. When criticality fields are displayed on a dashboard, the normalized values can then provide consistent information across object types.

Workflow stages

A workflow is made up of one start stage, one or many standard stages, and one or many end stages.

Defining a start stage

When you create a new workflow, a start stage is created for you. However, if you delete the default start stage, you must create another one because every workflow must have at least one start stage.

Procedure

1. Click  > **Solution Configuration** > **Workflows**.
2. Click  in the toolbar and drag it to the canvas.
3. In the **New Stage** window, give the stage a **Name** and click **Create**.

This is an internal name and it cannot be changed later. In the next step, you can define a label for the stage.

Allowed characters are A-Z, a-z, 0-9, underscore, hyphen, and spaces. Special characters are not allowed.

Maximum length is 40 characters. Keep the stage names short.

4. Enter a **Label** for the stage.

Allowed characters are A-Z, a-z, 0-9, underscore, hyphen, and spaces. Special characters are not allowed.

The label is populated to all languages.

If the workflow is used in multiple locales, enter a stage label for each language.

If it is displayed, click  to populate translated values to languages. For more information, see “IBM Watson Language Translator” on page 847.

Maximum length is 40 characters.

Keep the stage labels short, for example, In Progress, In Review, In Approval, and Closed. Stage labels are displayed in the workflow information card.

5. Ensure that the **Type** selected is **Start**.

Defining a standard stage

A workflow can have one or many standard stages.

Procedure

1. Click  > **Solution Configuration** > **Workflows**.
2. Click the workflow that you want to edit.
The GRC Workflow Designer opens.
3. Click  in the toolbar and drag it to the canvas.
4. In the **New Stage** window, give the stage a **Name** and click **Create**.

This is an internal name and it cannot be changed later. In the next step, you can define a label for the stage.

Allowed characters are A-Z, a-z, 0-9, underscore, hyphen, and spaces. Special characters are not allowed.

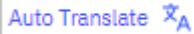
Maximum length is 40 characters. Keep the stage names short.

5. Enter a **Label** for the stage.

Allowed characters are A-Z, a-z, 0-9, underscore, hyphen, and spaces. Special characters are not allowed.

The label is populated to all languages.

If the workflow is used in multiple locales, enter a stage label for each language.

 Auto Translate

If it is displayed, click  to populate translated values to languages. For more information, see “IBM Watson Language Translator” on page 847.

Maximum length is 40 characters.

Keep the stage labels short, for example, In Progress, In Review, In Approval, and Closed. Stage labels are displayed in the workflow information card.

6. Choose **Standard** in **Type**.

7. In **Access Control**, define whether non-participants can view and edit objects at this stage.

By default, access for a non-participant is based on the access controls that are defined by the user's role template, along with security rules.

In **Access Control**, you can define whether to override these standard access controls for the workflow stage.

Table 142. Access controls for non-participants

Access control for the stage	Can view the object when it's at this stage	Can edit the object when it's at this stage	Can see the Actions button in views
Strict	No	No	No
Read	Yes	No	No
Open	Depends on standard access controls	Depends on standard access controls	No
No Override	Depends on standard access controls	Depends on standard access controls	Yes

Remember: For workflow participants (assignees, oversight users, and subscribers), the standard access controls determine whether they can view and edit the object. All workflow participants can see the **Actions** button.

8. In **Due Date** define the stage due date.

In **Assign To** choose how the stage due date is set.

- Start Date (the date when a workflow instance enters (or re-enters) the stage)
- A specified value
- A field in the current object
- **A field in a related object**
 - Select Direct Child, Direct Parent, Ancestor, or Descendant in **Relationship Type**.
 - Select an object type in **Related Object Type**.
 - Select a path in **Relationship Paths** (displays only if **Relationship Type** is Ancestor or Descendant).
 - Select a field in **Related Object Field**.
 - Add **Filter By** conditions (optional).
 - Set **Primary Parent Only** (displays only if **Relationship Type** is Direct Parent or Ancestor) (optional).

You can optionally add **Filter By** conditions and set **Advanced Logic**.

- A field in a Preference object

You can add optionally add **Filter By** conditions.

In **Adjust Date By** you can optionally define an offset for the date you chose in **Assign To**. The offset is always in days and can be negative. It can be:

- A specified value, for example, 10 days.
- A field in the current object
- **A field in a related object**
 - Select Direct Child, Direct Parent, Ancestor, or Descendant in **Relationship Type**.
 - Select an object type in **Related Object Type**.
 - Select a path in **Relationship Paths** (displays only if **Relationship Type** is Ancestor or Descendant).
 - Select a field in **Related Object Field**.
 - Add **Filter By** conditions (optional).
 - Set **Primary Parent Only** (displays only if **Relationship Type** is Direct Parent or Ancestor) (optional).

You can optionally add **Filter By** conditions and set **Advanced Logic**.

- A field in a Preference object

You can optionally add **Filter By** conditions.

Expand **Assignees and Subscribers** to designate the assignees and subscribers for tasks at this stage.

You can select only actor fields. Do not select a system workflow field such as *System Workflow Fields:Assignees*. You can assign multiple assignees and multiple subscribers to a stage. They can be from multiple sources, for example, a specific user, a field on the current object, and a field on a related object.

9. Click **Add Assignee** to designate the assignees for tasks at this stage. You can choose to:

Assign to

- Users or groups
- A field in the current object
- **A field in a related object**
 - Select Direct Child, Direct Parent, Ancestor, or Descendant in **Relationship Type**.
 - Select an object type in **Related Object Type**.
 - Select a path in **Relationship Paths** (displays only if **Relationship Type** is Ancestor or Descendant).
 - Select a field in **Related Object Field**.
 - Add **Filter By** conditions (optional).
 - Set **Primary Parent Only** (displays only if **Relationship Type** is Direct Parent or Ancestor) (optional).

You can optionally add **Filter By** conditions and set **Advanced Logic**.

- A field in a preference object

You can optionally add **Filter By** conditions.

10. Click **Add Subscriber** to designate the subscribers for tasks at this stage. You can choose to:

Assign to

- Users or groups
- A field in the current object

- **A field in a related object**

- Select Direct Child, Direct Parent, Ancestor, or Descendant in **Relationship Type**.
- Select an object type in **Related Object Type**.
- Select a path in **Relationship Paths** (displays only if **Relationship Type** is Ancestor or Descendant).
- Select a field in **Related Object Field**.
- Add **Filter By** conditions (optional).
- Set **Primary Parent Only** (displays only if **Relationship Type** is Direct Parent or Ancestor) (optional).

You can optionally add **Filter By** conditions and set **Advanced Logic**.

- A field in a Preference object

You can optionally add **Filter By** conditions.

11. Set **Enable Reminders** to true to send email reminders. Configure who receives reminders and when.

- a) Set **Send reminders to Assignees** to true or false.
- b) Set **Send reminders to Subscribers** to true or false.
- c) Configure how frequently email reminders are sent in the following settings.

Table 143. Reminder frequency settings

Setting	Description	Example
Send reminder __ day(s) before due date	A user receives one email reminder x days before the due date. Do not enter 0. Instead, set Send reminders on due date to true.	1= user receives one email reminder one day before the due date 3= user receives one email reminder three days before the due date
Send reminder every __ day(s) until due date	A user receives repeating email reminders every x days until the due date.	1= user receives an email reminder every day until the due date 3= user receives an email reminder every three days until the due date
Send reminders on due date (true/false)	If true, a user receives one email reminder on the due date.	
Send reminder every __ day(s) for overdue tasks	A user receives repeating email reminders every x days after the due date has passed. Emails are sent until the stage is completed.	1= user receives an email reminder every day after the due date has passed 3= user receives an email reminder every three days after the due date has passed

12. Optional: Expand **Bulk Workflow Action** to set **Bulk Workflow Action to True** to enable bulk workflow actions.

If you set **Bulk Workflow Action to True**, do the following steps:

- Select a Grid View in **Select a grid view for Bulk Workflow Action**. For more information, see “Defining a Grid View” on page 257.

- In **Enable Workflow Actions for Bulk Processing**, each action accessible from the current workflow stage is displayed. Turn on each action that you want to allow users to take during bulk workflow actions. Each activated action will be an option in the toolbar in the Grid View.

13. Expand **Task View Overrides** to provide overrides that customize the Task View that is displayed to the user for the stage.

- In **View** select a task view for the stage or leave blank.

If you provide a task view, you can also provide field, section, and user guidance overrides that customize the task view for the stage. The task view must be enabled.

If blank, the system uses information in the workflow and rules on the task views for the object type to determine the task view that is displayed.

- In **Fields** define field overrides for the task view. Click **Add Field**, choose a field, and set the following attributes:

Table 144. Field attributes

Attribute name	Settings	Description
Hidden	True or False	Overrides rules in the task view that determine whether the field is shown or hidden.
Read Only	True or False	Overrides rules in the task view that determine whether a field is read only.
Key Field	True or False	<p>Adds the field to the list of Key Fields in the user guidance panel, regardless of whether the user guidance is defined in the task view or the guidance text override.</p> <p>If a field is hidden in a view due to a task view override, it is also hidden in the user guidance panel if it is defined as a key field.</p> <p>For more information about key fields, see “Adding user guidance” on page 282.</p>

- In **Sections** define section overrides for the task view (optional). Click **Add Section**, choose a section, and set the following attributes:

Table 145.

Attribute name	Settings	Description
Hide Section	True or False	Controls whether the section is shown or hidden.
Initially Collapsed	True or False	Overrides the Initially Collapsed setting that is defined on the section in the task view.

For more information about sections, see “[Adding a section](#)” on page 278.

- Enter a **Guidance Title** to provide a title for the user guidance panel for the stage. The title is populated to all languages. Alternatively, you can enter titles for different languages.

- Enter **Guidance Text** to override the user guidance text on the task view. The text is populated to all languages. Alternatively, you can enter user guidance text for different languages. For more information about user guidance, see “[Adding user guidance](#)” on page 282.

Defining an end stage

A workflow must have at least one end stage.

Procedure

1. Click  > **Solution Configuration** > **Workflows**.

2. Click  in the toolbar and drag it to the canvas.

3. In the **New Stage** window, give the stage a **Name** and click **Create**.

This is an internal name and it cannot be changed later. In the next step, you can define a label for the stage.

Allowed characters are A-Z, a-z, 0-9, underscore, hyphen, and spaces. Special characters are not allowed.

Maximum length is 40 characters. Keep the stage names short.

4. Enter a **Label** for the stage.

Allowed characters are A-Z, a-z, 0-9, underscore, hyphen, and spaces. Special characters are not allowed.

The label is populated to all languages.

If the workflow is used in multiple locales, enter a stage label for each language.

If it is displayed, click  to populate translated values to languages. For more information, see “[IBM Watson Language Translator](#)” on page 847.

Maximum length is 40 characters.

Keep the stage labels short, for example, In Progress, In Review, In Approval, and Closed. Stage labels are displayed in the workflow information card.

5. For the **Type**, choose **End**.

In **End Stage Notifications**, designate who receives an email notification when the workflow ends.

You can also customize the templates for email notifications. For more information, see “[Customizing email notification templates in workflows](#)” on page 427.

6. Add other users who receive email notifications.

a) Click **Add User**.

You can assign to:

- **Users or groups**
- **A field in the current object**
- **A field in a related object**

– Select Direct Child, Direct Parent, Ancestor, or Descendant in **Relationship Type**.

– Select an object type in **Related Object Type**.

– Select a path in **Relationship Paths** (displays only if **Relationship Type** is Ancestor or Descendant).

– Select a field in **Related Object Field**.

– Add **Filter By** conditions (optional).

- Set **Primary Parent Only** (displays only if **Relationship Type** is Direct Parent or Ancestor) (optional).

You can optionally add **Filter By** conditions and set **Advanced Logic**.

- **A field in a preference object**

You can optionally add **Filter By** conditions and set **Advanced Logic**.

The panel changes depending on your selection.

- Complete the panel.
- Click **Done**.

In **Operations** click **New Operation** to define an operation that executes when the workflow ends. The only operation that is available is to start a workflow.

7. In **Operation** choose **start a workflow**. When the current workflow ends, another workflow immediately begins for the same object.
8. Provide a **Name** for the operation.
9. Click **New Condition** to add one or more conditions to the **start a workflow** operation. The **When** panel opens. For each condition you build a comparison statement with two fields and an operator.

- a) In **Compare**, you define the first field in the comparison statement. You can choose:

- **A field in the current object**

Select an **Object Field**.

- **A field in a related object**

- Select Direct Child, Direct Parent, Ancestor, or Descendant in **Relationship Type**.
- Select an object type in **Related Object Type**.
- Select a field in **Related Object Field**.
- Select a path in **Relationship Paths** (displays only if **Relationship Type** is Ancestor or Descendant).
- Add **Filter By** conditions (optional).
- Set **Primary Parent Only** (displays only if **Relationship Type** is Direct Parent or Ancestor) (optional).

- **A field in a Preference object**

Select a **Preference Object Field**. You can add **Filter By** conditions.

- **End User**

An **End User** condition checks whether the signed on end user is a specified user and whether the user is in a specified user group. The second field in the comparison statement is a specified value, an expression, or an actor field on an object.

- b) In **Using**, choose an **Operator**. The list of operators depends on the field type of the field you chose in **Compare**.

- c) In **To**, you define the second field in the comparison statement. You can choose:

- **A specified value**

The value that you can provide depends on the field type of the field you chose in **Compare**. The comparison is case sensitive, so ensure that you specify the correct case for the value.

- **An expression**

Enter a single field or variable from the list in “[Using variables, functions, and fields](#)” on page [377](#). All of the variables and fields listed there can be used in an expression. The field or variable must be in the given format. It can, however, be part of a longer string, for example, a file name like Evidence_[\$Parent:SOXRisk/System Fields:Name\$].pdf if you want to validate that the parent object has a specific PDF attachment.

- **A field in the current object**

Select an **Object Field**.

- **A field in a related object**

- Select **Direct Child, Direct Parent, Ancestor, or Descendant** in **Relationship Type**.
- Select an object type in **Related Object Type**.
- Select a field in **Related Object Field**.
- Select a path in **Relationship Paths** (displays only if **Relationship Type** is Ancestor or Descendant).
- Add **Filter By** conditions (optional).
- Set **Primary Parent Only** (displays only if **Relationship Type** is Direct Parent or Ancestor) (optional).

- **A field in a Preference object**

Select a **Preference Object Field**. You can add **Filter By** conditions.

d) If you chose a date field in **Compare**, you can define an offset in **Adjust Date By**.

- **A specified value** and enter **Number of Days**.

- **A field in the current object**

- **A field in a related object**

- Select Direct Child, Direct Parent, Ancestor, or Descendant in **Relationship Type**.
- Select an object type in **Related Object Type**.
- Select a field in **Related Object Field**.
- Select a path in **Relationship Paths** (displays only if **Relationship Type** is Ancestor or Descendant).
- Add **Filter By** conditions (optional).
- Set **Primary Parent Only** (displays only if **Relationship Type** is Direct Parent or Ancestor) (optional).

- **A field in the Preference object**

You can add **Filter By** conditions.

e) Click **Done**.

The condition is saved and assigned a number. Conditions are numbered consecutively in the order they are defined.

f) Optional: Add more conditions.

g) Optional: Set **Advanced Logic** to true to override the default rule that all conditions must be met. Write a statement in **Logic**. Use the condition numbers together with the operators and, or, not, and parentheses.

The order of operations is: () then NOT then AND then OR.

For example:

- 1 or 2 or 3
- 1 and (2 or 3)
- 1 not (2 or 3)

10. **Target Objects** defaults to Self and cannot be changed.

11. In **Workflow** enter the name of the workflow to start. The workflow must be for the same object type as the workflow that is ending. It must be published.

12. Click **Done**.

Deleting stages

In the GRC Workflow Designer, you can delete stages.

Procedure

To delete a stage from a workflow, choose one of the following options:

- Select a stage on the canvas and press Delete on the keyboard.
- Select a stage on the canvas and click **Delete Stage** in the stage property panel.

Workflow actions

Actions control aspects of the transition to the next or previous stage.

Conditions and validations

You use conditions and validations to customize the presentation to the user and to define the behavior of a workflow. The options for conditions and validations are the same. The difference between conditions and validations is their effect on the behavior of the Task View when a user completes their work.

- You can use conditions to restrict the list of actions that are visible to users. Conditions can hide branches of the workflow based on the values of the current object's fields, or the values of fields on related objects. The following list shows some examples of how you can use conditions:
 - You can define a condition that displays **Escalation** on the **Actions** button if the loss amount is greater than \$1M.
 - You can define a condition that hides **Submit** on the **Actions** button if given fields are empty.
 - You can define a condition that hides **Submit** on the **Actions** button if all related action items are not closed.

If the action has **Auto-Advance Stage** set to **True**, the conditions control whether the action advances the workflow to the next stage as in the following examples:

- You can define an auto-advance action that progresses to the next stage when a user saves the object with a specified set of field values. If the user saves an object with a loss amount greater than \$1 M, it can automatically take the Escalation action.
- You can use auto-advance conditions to create a branch node that automatically picks the correct workflow path based on an object's field value. If there have two types of issues, IT and OR, the workflow takes the correct branch based on the condition on the issue type. The user follows the workflow for their issue type and is unaware of the other issue type.
- Validations check that an object has specific attributes for the action to complete. If the validation fails, an error is displayed and the user must take corrective steps. Examples include:
 - You can define a validation that makes certain fields mandatory when the user clicks **Escalation**. If the fields are empty, an error is displayed. The user must provide values to continue.
 - You can define a validation that requires all related action items be closed. If they are not closed, the user must close them to continue.

Operations

Operations control what is done when the action completes. For example, when an object is approved, you can create an object, start another workflow, or set a date field to today's date.

An action can complete the following types of operations:

- Create objects.
- Run a custom action.
- Lock or unlock objects.

- Set fields.
- Start a workflow.

Order of validations and operations

Validations and operations are performed in the order given. For example, an action can perform a validation, then an operation, and then another validation.

Initial and final actions

The first action in a workflow is from the start stage to the first standard stage. This action occurs automatically without user input. You can use this action to define initial properties for the workflow. If the workflow has multiple first standard stages, each action from the start stage to the standard stage must have a condition.

The final action in a workflow is from the last standard stage to the end stage. You can use this action to reset any field values, if needed, and to define fields you need for the next workflow, if there is one.

Auto-advancing to the next stage

You can set actions so that the workflow automatically advances to the next stage when the user arrives at the originating stage. For example, in Figure 1, **Action 3** has the **Auto-Advance Stage** property set to **True**. When the workflow is on **Stage 1**, the user selects an option on the **Actions** button to advance to **Stage 2**. Because **Action 3** is set to auto-advance and **Action 3** is the final action, the workflow advances to the **End** stage automatically.

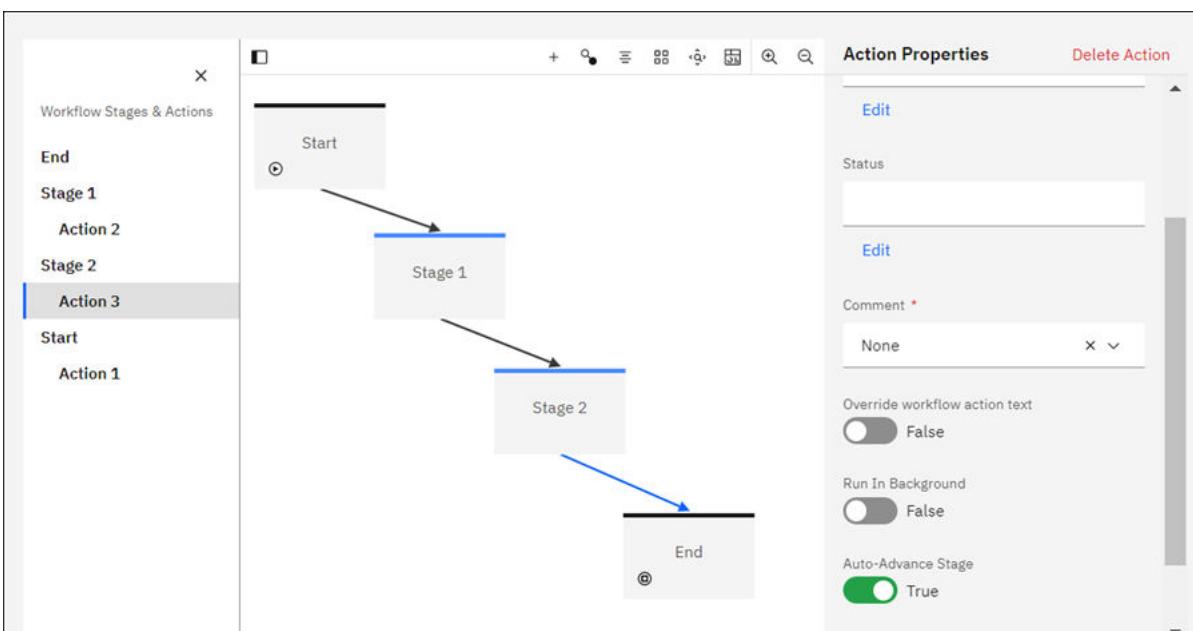


Figure 58. Setting an action to auto-advance

Operations and validations

You can configure operations and validations on an automatic action. If an operation or validation fails, the workflow goes back to the last stage where the user selected an option on the **Actions** button. In Figure 1, if an operation on the automatic transition fails on **Action 3**, the workflow goes back to **Stage 1** and an error is displayed.

Conditions

You can define conditions on automatic actions. All conditions on the action must be true to advance to the next stage. If any of the conditions are not true, the workflow waits until the object is in a state where

the conditions are met. If you have more than one automatic action, only one of the actions can have all true conditions; otherwise, an error is displayed.

An automatic action will not advance to the next stage if it has one of the following conditions:

- A condition that uses a system variable, such as `[END_USER]` or `[$TODAY$]`, in an expression.
- A condition that uses a setting other than **A field in the current object** in the **Compare** section.

Defining a workflow action

About this task

You can connect two stages with one action, for example, an action that represents an approval. The line between the two stages is shown with one arrowhead. When you click the line, the properties for the action are displayed in the property panel.

You can also connect two stages with two actions, for example, an action that represents an approval and one that represents a rejection. Draw the first action in one direction, and then draw the second action in the opposite direction. The result is a single line with two arrowheads. When you click an arrowhead, the properties for the selected action are displayed in the property panel. Use the property panel to verify that the correct action is selected.

In **Validations and Operations** you can add one or more validations and one or more operations. They are performed in the order given. Drag the validations and operations up or down to place them in the correct order for processing.

Note: Do not use the System Comment field (System Fields:Comment) in workflows. This system field is a special field that is used with File (SOXDocument) and Signature objects.

Procedure

1. Click  > **Solution Configuration** > **Workflows**.
2. Click the workflow that you want to edit.
The GRC Workflow Designer opens.
3. To create an action, click the stage where the action starts. Four points are activated on the stage. Grab a point and pull a line to the stage where the action ends.
4. In the **New Action** window, keep the default or give the action a **Name** and click **Create**.

Name is an internal name and it cannot be changed later. The name must be unique within a stage. In the next step, you can define a label.

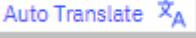
Allowed characters are A-Z, a-z, 0-9, underscore, hyphen, and spaces. Special characters are not allowed.

The **Action Properties** panel opens.

5. In **Label** enter a label for the action. The default is the **Name**.

Allowed characters are A-Z, a-z, 0-9, underscore, hyphen, and spaces. Special characters are not allowed.

The **Name** is populated to labels for other languages. Click **Edit** and overwrite the labels if the workflow is used in multiple locales.

If it is displayed, click  to populate translated values to languages. For more information, see “IBM Watson Language Translator” on page 847.

Workflow labels are displayed on the dashboard, **My Tasks** tab, **Subscription Tasks** tab, and **Oversight Tasks** tab.

Action labels are displayed as options under **Actions**.

Keep the action labels short, for example, Submit for review, Reject, Send for approval, Reject approval, and Approve and close.

6. In **Status**, enter a status that is assigned to the next stage in the workflow. The value is populated to all languages. Alternatively, choose a language and enter a value for that language. You can enter values for multiple languages.

If it is displayed, click  to populate translated values to languages. For more information, see [“IBM Watson Language Translator” on page 847](#).

Statuses are usually displayed in the workflow information card as stage label [status label], for example, *In Review [Rejected]*. However, for the action to the end stage, the status of the end stage is not displayed in the information card.

There is no automatic link between the **Status** field on a workflow and any status fields that can exist on an object, for example, the Business Continuity Plan status field (BC-Plan:Status). Use a **Set fields** operation on an action to control the value in object status fields as objects move through a workflow.

7. In **Comment** you can control how the action handles a user-entered comment. Options are:

- **None** - no comment is allowed and a comment window is not displayed.
- **Optional** - a comment window is displayed and a user can enter a comment. However, the comment is not required for the action to complete.
- **Required** - a comment window is displayed and a user must enter a comment for the action to complete.

The **Comment** setting is hidden for the initial action in a workflow (from the start stage to the first standard stage).

Note: Information in workflow system fields, including user-entered action comments, is only accessible when the workflow is in progress. Once the workflow completes, these workflow fields are no longer available. If you want to retain the value in that field, you can use the workflow **Set field** operation to save the value to a non-workflow field.

8. In **Override workflow action text** provide text that displays on the confirmation window that users interact with. For more information, see [“Confirm the selected action” on page 375](#).

9. Set **Run in Background** to **True** if the action is expected to take a long time.

10. Set **Auto-Advance Stage** to **True** so that the workflow automatically processes the action when the user reaches the originating stage.

11. If the action doesn't end with an end stage, the **Email** properties section is displayed. Expand the **Email** section, and set the following options to **True** to send email notifications when the action completes:

- **Notify Assignees**

When you set **Notify Assignees** to **True**, the **Customize** link is displayed so that you can customize the assignee subject and body templates for email notifications.

- **Notify Subscribers**

When you set **Notify Subscribers** to **True**, the **Customize** link is displayed so that you can customize the subscriber subject and body templates for email notifications.

For more information about customizing email notifications, see [“Customizing email notification templates in workflows” on page 427](#).

If **Run in Background** is set to **True**, email notifications that are related to the completion of the action are not impacted by the settings for emails that are sent to Assignees and Subscribers.

12. Expand **Conditions** and click **New Condition**. The **Conditions** panel opens.

Conditions control whether an action is visible or hidden on the **Actions** button. Conditions provide a means for you to restrict options available to users and hide the workflow and its complexity.

You can add one or more conditions. For each condition, you build a comparison statement with two fields and an operator.

All conditions must be met for the action on the **Actions** button to display.

To override this rule, define **Advanced Logic** to combine the conditions in a specific way.

a) In **Compare**, you define the first field in the comparison statement. You can choose:

- **A field in the current object**

Select an **Object Field**.

- **A field in a related object**

- Select Direct Child, Direct Parent, Ancestor, or Descendant in **Relationship Type**.
- Select an object type in **Related Object Type**.
- Select a field in **Related Object Field**.
- Select a path in **Relationship Paths** (displays only if **Relationship Type** is Ancestor or Descendant).
- Add **Filter By** conditions (optional).
- Set **Primary Parent Only** (displays only if **Relationship Type** is Direct Parent or Ancestor) (optional).

- **A field in a Preference object**

Select a **Preference Object Field**. You can add **Filter By** conditions.

- **End User**

An **End User** condition checks whether the signed on end user is a specified user and whether the user is in a specified user group. The second field in the comparison statement is a specified value, an expression, or an actor field on an object.

b) In **Using**, choose an **Operator**. The list of operators depends on the field type of the field you chose in **Compare**.

c) In **To**, you define the second field in the comparison statement. You can choose:

- **A specified value**

The value that you can provide depends on the field type of the field you chose in **Compare**. The comparison is case sensitive, so ensure that you specify the correct case for the value.

- **An expression**

Enter a single field or variable from the list in “[Using variables, functions, and fields](#)” on page 377. All of the variables and fields listed there can be used in an expression. The field or variable must be in the given format. It can, however, be part of a longer string, for example, a file name like Evidence_[\$Parent:SOXRisk/System Fields:Name\$].pdf if you want to validate that the parent object has a specific PDF attachment.

- **A field in the current object**

Select an **Object Field**.

- **A field in a related object**

- Select **Direct Child, Direct Parent, Ancestor, or Descendant** in **Relationship Type**.
- Select an object type in **Related Object Type**.
- Select a field in **Related Object Field**.
- Select a path in **Relationship Paths** (displays only if **Relationship Type** is Ancestor or Descendant).
- Add **Filter By** conditions (optional).
- Set **Primary Parent Only** (displays only if **Relationship Type** is Direct Parent or Ancestor) (optional).

- **A field in a Preference object**

Select a **Preference Object Field**. You can add **Filter By** conditions.

- d) If you chose a date field in **Compare**, you can define an offset in **Adjust Date By**.

- **A specified value** and enter **Number of Days**.

- **A field in the current object**

- **A field in a related object**

- Select Direct Child, Direct Parent, Ancestor, or Descendant in **Relationship Type**.

- Select an object type in **Related Object Type**.

- Select a field in **Related Object Field**.

- Select a path in **Relationship Paths** (displays only if **Relationship Type** is Ancestor or Descendant).

- Add **Filter By** conditions (optional).

- Set **Primary Parent Only** (displays only if **Relationship Type** is Direct Parent or Ancestor) (optional).

- **A field in the Preference object**

You can add **Filter By** conditions.

- e) Click **Done**.

The condition is saved and assigned a number. Conditions are numbered consecutively in the order they are defined.

- f) Optional: Add more conditions.

- g) Optional: Set **Advanced Logic** to true to override the default rule that all conditions must be met.

Write a statement in **Logic**. Use the condition numbers together with the operators and, or, not, and parentheses.

The order of operations is: () then NOT then AND then OR.

For example:

- 1 or 2 or 3
- 1 and (2 or 3)
- 1 not (2 or 3)

13. Expand **Validations and Operations** and click **New Validation** to define a validation. The **Validations** panel opens.

In **Validation Type**, select either **Simple Validation** or **Advanced Logic**.

Validations check that an object has specific attributes for the action to complete. If the validation fails, an error is displayed and the user must take corrective steps.

In **Custom error message**, enter the text that appears in an error message when the validation condition is not true. When the message is displayed, it shows the message ID, the text you entered in the **Custom error message** field, and the data and time when the error occurred. The maximum number of characters for a custom error message is 196. You can enter plain text only for a custom error message; HTML is not supported.

The error is also recorded in the log file <server_name>Server</>-aurora.log. The original error message appears in the log rather than the custom error message. For more information about this and other log files on application servers, see “[Log files on application servers](#)” on page 696.

All validations must be met for the action to complete. For each validation you build a comparison statement with two fields and an operator.

- a) In **Compare**, you define the first field in the comparison statement. You can choose:

- **A field in the current object**

Select an **Object Field**.

- **A field in a related object**

- Select Direct Child, Direct Parent, Ancestor, or Descendant in **Relationship Type**.
- Select an object type in **Related Object Type**.
- Select a field in **Related Object Field**.
- Select a path in **Relationship Paths** (displays only if **Relationship Type** is Ancestor or Descendant).
- Add **Filter By** conditions (optional).
- Set **Primary Parent Only** (displays only if **Relationship Type** is Direct Parent or Ancestor) (optional).

- **A field in a Preference object**

Select a **Preference Object Field**. You can add **Filter By** conditions.

- **End User**

An **End User** condition checks whether the signed on end user is a specified user and whether the user is in a specified user group. The second field in the comparison statement is a specified value, an expression, or an actor field on an object.

- b) In **Using**, choose an **Operator**. The list of operators depends on the field type of the field you chose in **Compare**.
- c) In **To**, you define the second field in the comparison statement. You can choose:

- **A specified value**

The value that you can provide depends on the field type of the field you chose in **Compare**. The comparison is case sensitive, so ensure that you specify the correct case for the value.

- **An expression**

Enter a single field or variable from the list in “[Using variables, functions, and fields](#)” on page 377. All of the variables and fields listed there can be used in an expression. The field or variable must be in the given format. It can, however, be part of a longer string, for example, a file name like Evidence_[**\$Parent:SOXRisk/System Fields:Name\$**].pdf if you want to validate that the parent object has a specific PDF attachment.

- **A field in the current object**

Select an **Object Field**.

- **A field in a related object**

- Select **Direct Child**, **Direct Parent**, **Ancestor**, or **Descendant** in **Relationship Type**.
- Select an object type in **Related Object Type**.
- Select a field in **Related Object Field**.
- Select a path in **Relationship Paths** (displays only if **Relationship Type** is Ancestor or Descendant).
- Add **Filter By** conditions (optional).
- Set **Primary Parent Only** (displays only if **Relationship Type** is Direct Parent or Ancestor) (optional).

- **A field in a Preference object**

Select a **Preference Object Field**. You can add **Filter By** conditions.

- d) If you chose a date field in **Compare**, you can define an offset in **Adjust Date By**.

- **A specified value** and enter **Number of Days**.

- **A field in the current object**

- **A field in a related object**

- Select Direct Child, Direct Parent, Ancestor, or Descendant in **Relationship Type**.
- Select an object type in **Related Object Type**.
- Select a field in **Related Object Field**.
- Select a path in **Relationship Paths** (displays only if **Relationship Type** is Ancestor or Descendant).
- Add **Filter By** conditions (optional).
- Set **Primary Parent Only** (displays only if **Relationship Type** is Direct Parent or Ancestor) (optional).

- **A field in the Preference object**

You can add **Filter By** conditions.

e) Click **Done**.

The condition is saved and assigned a number. Conditions are numbered consecutively in the order they are defined.

f) Optional: Add more conditions.

g) Optional: Set **Advanced Logic** to true to override the default rule that all conditions must be met. Write a statement in **Logic**. Use the condition numbers together with the operators and, or, not, and parentheses.

The order of operations is: () then NOT then AND then OR.

For example:

- 1 or 2 or 3
- 1 and (2 or 3)
- 1 not (2 or 3)

14. Expand **Validations and Operations** and click **New Operation** to define an operation. The **Operations** panel opens.

Operations define what is done when the action completes.

If you provide multiple operations, all operations are performed.

a) In **Operation** choose an operation type. Valid values are:

- Create objects
- Custom action
- Lock or unlock objects
- Set fields
- Start a workflow

The fields on the **Operations** panel change depending on the operation type you choose.

b) Follow the instructions for the operation type. For more information see:

- [“Defining a workflow action that creates objects” on page 413](#)
- [“Defining a workflow action that runs a custom action ” on page 415](#)
- [“Defining a workflow action that locks or unlocks objects” on page 417](#)
- [“Defining a workflow action that sets fields” on page 420](#)
- [“Defining a workflow action that starts a workflow” on page 422](#)
- [“Defining a workflow action that runs a calculation” on page 425](#)

15. If you provide multiple validations or operations, review the order. Validations and operations are executed in the order given.

What to do next

Depending on the workflow, you might need to define an action back to the previous stage.

Repeat the step of creating an action but in the reverse direction. The result is a single line with two arrowheads. When you click an arrowhead, the properties for the selected action are displayed in the property panel. Use the property panel to verify that you have the correct action selected.

Defining a workflow action that creates objects

A **create objects** operation on an action creates a single direct child object.

Before you begin

Define a workflow and add stages and actions to it. For information about how to define an action, “[Defining a workflow action](#)” on page 407.

Review “[Designing a workflow](#)” on page 379. Be aware of the potential of creating an infinite loop when defining a workflow action that creates objects.

Procedure

1. In the GRC Workflow Designer, click the action that you want to edit.
The **Action Properties** panel opens.
2. Expand **Validations and Operations**.
3. Click **New Operation**. The **Operations** panel opens.
4. Set **Operation to create objects**.
5. Provide a **Name** for the operation.
6. Next to **When**, click **New Condition** to define one or more conditions. The **When** panel opens.

All conditions must be met for the operation to complete. For each condition you build a comparison statement with two fields and an operator.

- a) In **Compare**, you define the first field in the comparison statement. You can choose:
 - **A field in the current object**
Select an **Object Field**.
 - **A field in a related object**
 - Select Direct Child, Direct Parent, Ancestor, or Descendant in **Relationship Type**.
 - Select an object type in **Related Object Type**.
 - Select a field in **Related Object Field**.
 - Select a path in **Relationship Paths** (displays only if **Relationship Type** is Ancestor or Descendant).
 - Add **Filter By** conditions (optional).
 - Set **Primary Parent Only** (displays only if **Relationship Type** is Direct Parent or Ancestor) (optional).
 - **A field in a Preference object**
Select a **Preference Object Field**. You can add **Filter By** conditions.
 - **End User**
An **End User** condition checks whether the signed on end user is a specified user and whether the user is in a specified user group. The second field in the comparison statement is a specified value, an expression, or an actor field on an object.
- b) In **Using**, choose an **Operator**. The list of operators depends on the field type of the field you chose in **Compare**.
- c) In **To**, you define the second field in the comparison statement. You can choose:
 - **A specified value**

The value that you can provide depends on the field type of the field you chose in **Compare**. The comparison is case sensitive, so ensure that you specify the correct case for the value.

- **An expression**

Enter a single field or variable from the list in “[Using variables, functions, and fields](#)” on page 377. All of the variables and fields listed there can be used in an expression. The field or variable must be in the given format. It can, however, be part of a longer string, for example, a file name like Evidence_[\\$Parent:SOXRisk/System Fields:Name\$].pdf if you want to validate that the parent object has a specific PDF attachment.

- **A field in the current object**

Select an **Object Field**.

- **A field in a related object**

- Select **Direct Child, Direct Parent, Ancestor, or Descendant** in **Relationship Type**.
- Select an object type in **Related Object Type**.
- Select a field in **Related Object Field**.
- Select a path in **Relationship Paths** (displays only if **Relationship Type** is Ancestor or Descendant).
- Add **Filter By** conditions (optional).
- Set **Primary Parent Only** (displays only if **Relationship Type** is Direct Parent or Ancestor) (optional).

- **A field in a Preference object**

Select a **Preference Object Field**. You can add **Filter By** conditions.

d) If you chose a date field in **Compare**, you can define an offset in **Adjust Date By**.

- **A specified value and enter Number of Days**.

- **A field in the current object**

- **A field in a related object**

- Select Direct Child, Direct Parent, Ancestor, or Descendant in **Relationship Type**.
- Select an object type in **Related Object Type**.
- Select a field in **Related Object Field**.
- Select a path in **Relationship Paths** (displays only if **Relationship Type** is Ancestor or Descendant).
- Add **Filter By** conditions (optional).
- Set **Primary Parent Only** (displays only if **Relationship Type** is Direct Parent or Ancestor) (optional).

- **A field in the Preference object**

You can add **Filter By** conditions.

e) Click **Done**.

The condition is saved and assigned a number. Conditions are numbered consecutively in the order they are defined.

f) Optional: Add more conditions.

g) Optional: Set **Advanced Logic** to true to override the default rule that all conditions must be met. Write a statement in **Logic**. Use the condition numbers together with the operators and, or, not, and parentheses.

The order of operations is: () then NOT then AND then OR.

For example:

- 1 or 2 or 3

- 1 and (2 or 3)
 - 1 not (2 or 3)
7. Set **Execute As System** to **False** to execute the action as the logged in user. Set **Execute As System** to **True** to execute the action as the OPSSystem user. The action can then perform operations that the logged in user cannot. The history on the **Activity** tab shows OPSSystem as the user who performed the action.
- When you set **Execute As System** to **True**, all set field operations where **Target Objects** is set to **Self** are also executed as the OPSSystem user.
8. Choose a **Related Object Type**. You can choose only from child object types of the object type for the workflow.
9. Enter an **Object Name** to assign to the newly created object. It is not displayed for all object types or if auto naming is enabled. If auto naming is not enabled, once a workflow creates an object the workflow cannot be started again for the same object.
- Tip:** If **Object Name** is displayed, you can add the `[$TODAY$]` expression to make it unique per day. For example, if you enter `Auto_Issue_[$TODAY$]`, the newly created object is named `Auto_Issue_07182019`.
10. Add **Fields** and set their values on the newly created object.
11. Click **Done**.

Results

When the action takes place, a new object is created and the workflow continues to the next stage. If an auto-start workflow exists for the child object type and the applicability conditions are met, a workflow starts for the newly created object. Both workflow, the one for the parent and the one for the child, continue and are independent of each other.

Defining a workflow action that runs a custom action

Use **custom action** to define custom business logic for an action.

Before you begin

Define a workflow and add stages and actions to it. For information about how to define an action, [“Defining a workflow action” on page 407](#).

About this task

Custom actions are a means to implement workflows that have similar functionality to triggers in OpenPages. The action is evaluated during an action and `customaction` class is instantiated and executed.

For more information, see [Appendix E, “Creating custom actions for GRC workflows,” on page 957](#).

Procedure

1. In the GRC Workflow Designer, click the action that you want to edit.
The **Action Properties** panel opens.
2. Expand **Validations and Operations**.
3. Click **New Operation**. The **Operations** panel opens.
4. Set **Operation** to **Custom action**.
5. Provide a **Name** for the operation.
6. Next to **When**, click **New Condition** to define one or more conditions. The **When** panel opens.
All conditions must be met for the operation to complete. For each condition you build a comparison statement with two fields and an operator.
 - a) In **Compare**, you define the first field in the comparison statement. You can choose:

- **A field in the current object**

Select an **Object Field**.

- **A field in a related object**

- Select Direct Child, Direct Parent, Ancestor, or Descendant in **Relationship Type**.
- Select an object type in **Related Object Type**.
- Select a field in **Related Object Field**.
- Select a path in **Relationship Paths** (displays only if **Relationship Type** is Ancestor or Descendant).
- Add **Filter By** conditions (optional).
- Set **Primary Parent Only** (displays only if **Relationship Type** is Direct Parent or Ancestor) (optional).

- **A field in a Preference object**

Select a **Preference Object Field**. You can add **Filter By** conditions.

- **End User**

An **End User** condition checks whether the signed on end user is a specified user and whether the user is in a specified user group. The second field in the comparison statement is a specified value, an expression, or an actor field on an object.

b) In **Using**, choose an **Operator**. The list of operators depends on the field type of the field you chose in **Compare**.

c) In **To**, you define the second field in the comparison statement. You can choose:

- **A specified value**

The value that you can provide depends on the field type of the field you chose in **Compare**. The comparison is case sensitive, so ensure that you specify the correct case for the value.

- **An expression**

Enter a single field or variable from the list in “[Using variables, functions, and fields](#)” on page 377. All of the variables and fields listed there can be used in an expression. The field or variable must be in the given format. It can, however, be part of a longer string, for example, a file name like Evidence_[\$Parent:SOXRisk/System Fields:Name\$].pdf if you want to validate that the parent object has a specific PDF attachment.

- **A field in the current object**

Select an **Object Field**.

- **A field in a related object**

- Select **Direct Child, Direct Parent, Ancestor, or Descendant** in **Relationship Type**.
- Select an object type in **Related Object Type**.
- Select a field in **Related Object Field**.
- Select a path in **Relationship Paths** (displays only if **Relationship Type** is Ancestor or Descendant).
- Add **Filter By** conditions (optional).
- Set **Primary Parent Only** (displays only if **Relationship Type** is Direct Parent or Ancestor) (optional).

- **A field in a Preference object**

Select a **Preference Object Field**. You can add **Filter By** conditions.

d) If you chose a date field in **Compare**, you can define an offset in **Adjust Date By**.

- **A specified value** and enter **Number of Days**.

- **A field in the current object**

- **A field in a related object**

- Select Direct Child, Direct Parent, Ancestor, or Descendant in **Relationship Type**.
- Select an object type in **Related Object Type**.
- Select a field in **Related Object Field**.
- Select a path in **Relationship Paths** (displays only if **Relationship Type** is Ancestor or Descendant).
- Add **Filter By** conditions (optional).
- Set **Primary Parent Only** (displays only if **Relationship Type** is Direct Parent or Ancestor) (optional).

- **A field in the Preference object**

You can add **Filter By** conditions.

e) Click **Done**.

The condition is saved and assigned a number. Conditions are numbered consecutively in the order they are defined.

f) Optional: Add more conditions.

g) Optional: Set **Advanced Logic** to true to override the default rule that all conditions must be met. Write a statement in **Logic**. Use the condition numbers together with the operators and, or, not, and parentheses.

The order of operations is: () then NOT then AND then OR.

For example:

- 1 or 2 or 3
- 1 and (2 or 3)
- 1 not (2 or 3)

7. Set **Execute As System** to **False** to execute the action as the logged in user. Set **Execute As System** to **True** to execute the action as the OPSSystem user. The action can then perform operations that the logged in user cannot. The history on the **Activity** tab shows OPSSystem as the user who performed the action.

When you set **Execute As System** to **True**, all set field operations where **Target Objects** is set to **Self** are also executed as the OPSSystem user.

8. Enter a **Class Name**.

9. You can provide one or more properties. A property is a Name/Value pair. An example of a Name/Value pair is **ObjectType/SOXProcess**. Both Name and Value must be strings.

10. Click **Add Fields** and designate fields that are passed to the custom action.

11. Click **Done**.

Defining a workflow action that locks or unlocks objects

A **lock or unlock objects** operation on an action locks or unlocks either the object that a workflow is processing or one or more related objects.

Note: You can't use a workflow action to unlock the current object because a workflow can't start on a locked object. You must unlock an object before a workflow on that object can start.

Before you begin

Define a workflow and add stages and actions to it. For information about how to define an action, [“Defining a workflow action” on page 407](#).

Procedure

1. In the GRC Workflow Designer, click the action that you want to edit.

The **Action Properties** panel opens.

2. Expand **Validations and Operations**.

3. Click **New Operation**. The **Operations** panel opens.

4. Set **Operation** to **lock or unlock objects**.

5. Provide a **Name** for the operation.

6. Next to **When**, click **New Condition** to define one or more conditions. The **When** panel opens.

All conditions must be met for the operation to complete. For each condition you build a comparison statement with two fields and an operator.

a) In **Compare**, you define the first field in the comparison statement. You can choose:

- **A field in the current object**

Select an **Object Field**.

- **A field in a related object**

– Select Direct Child, Direct Parent, Ancestor, or Descendant in **Relationship Type**.

– Select an object type in **Related Object Type**.

– Select a field in **Related Object Field**.

– Select a path in **Relationship Paths** (displays only if **Relationship Type** is Ancestor or Descendant).

– Add **Filter By** conditions (optional).

– Set **Primary Parent Only** (displays only if **Relationship Type** is Direct Parent or Ancestor) (optional).

- **A field in a Preference object**

Select a **Preference Object Field**. You can add **Filter By** conditions.

- **End User**

An **End User** condition checks whether the signed on end user is a specified user and whether the user is in a specified user group. The second field in the comparison statement is a specified value, an expression, or an actor field on an object.

b) In **Using**, choose an **Operator**. The list of operators depends on the field type of the field you chose in **Compare**.

c) In **To**, you define the second field in the comparison statement. You can choose:

- **A specified value**

The value that you can provide depends on the field type of the field you chose in **Compare**. The comparison is case sensitive, so ensure that you specify the correct case for the value.

- **An expression**

Enter a single field or variable from the list in “[Using variables, functions, and fields](#)” on page 377. All of the variables and fields listed there can be used in an expression. The field or variable must be in the given format. It can, however, be part of a longer string, for example, a file name like Evidence_[**\$Parent:SOXRisk/System Fields:Name\$**].pdf if you want to validate that the parent object has a specific PDF attachment.

- **A field in the current object**

Select an **Object Field**.

- **A field in a related object**

– Select **Direct Child, Direct Parent, Ancestor, or Descendant** in **Relationship Type**.

– Select an object type in **Related Object Type**.

– Select a field in **Related Object Field**.

- Select a path in **Relationship Paths** (displays only if **Relationship Type** is Ancestor or Descendant).
- Add **Filter By** conditions (optional).
- Set **Primary Parent Only** (displays only if **Relationship Type** is Direct Parent or Ancestor) (optional).

- **A field in a Preference object**

Select a **Preference Object Field**. You can add **Filter By** conditions.

d) If you chose a date field in **Compare**, you can define an offset in **Adjust Date By**.

- **A specified value** and enter **Number of Days**.
- **A field in the current object**
- **A field in a related object**
 - Select Direct Child, Direct Parent, Ancestor, or Descendant in **Relationship Type**.
 - Select an object type in **Related Object Type**.
 - Select a field in **Related Object Field**.
 - Select a path in **Relationship Paths** (displays only if **Relationship Type** is Ancestor or Descendant).
 - Add **Filter By** conditions (optional).
 - Set **Primary Parent Only** (displays only if **Relationship Type** is Direct Parent or Ancestor) (optional).

- **A field in the Preference object**

You can add **Filter By** conditions.

e) Click **Done**.

The condition is saved and assigned a number. Conditions are numbered consecutively in the order they are defined.

f) Optional: Add more conditions.

g) Optional: Set **Advanced Logic** to true to override the default rule that all conditions must be met. Write a statement in **Logic**. Use the condition numbers together with the operators and, or, not, and parentheses.

The order of operations is: () then NOT then AND then OR.

For example:

- 1 or 2 or 3
- 1 and (2 or 3)
- 1 not (2 or 3)

7. Set **Execute As System** to **False** to execute the action as the logged in user. Set **Execute As System** to **True** to execute the action as the OPSystem user. The action can then perform operations that the logged in user cannot. The history on the **Activity** tab shows OPSystem as the user who performed the action.

When you set **Execute As System** to **True**, all set field operations where **Target Objects** is set to **Self** are also executed as the OPSystem user.

8. Click **Edit** next to **Target Objects**. Establish what objects are locked or unlocked.

a. Select a **Relationship Type**:

- Self
- Direct Child
- Direct Parent
- Ancestor

- Descendant
 - b. Select a **Related Object Type** if you chose any value other than Self. The list is filtered based on what you chose in **Relationship Type**.
 - c. Click **New Condition** to add a condition to the target object.
 - d. If you chose Ancestor or Descendant in **Relationship Type**, select a path in **Relationship Paths**.
 - e. Click **Done**.
9. In **Lock/unlock** choose lock or unlock.
10. Click **Done**.

Defining a workflow action that sets fields

A **set fields** operation on an action sets values for specified fields on either the object that a workflow is processing or one or more related objects.

Before you begin

Define a workflow and add stages and actions to it. For information about how to define an action, “[Defining a workflow action](#)” on page 407.

About this task

If a **set fields** operation sets a field on a child object, conditional on another field on that child object, the action works only if all children meet the condition. If any child object does not meet the condition, then no changes are made to any child. A solution for this is to add a **Filter by** condition on the **When** panel so that only a subset of children are included.

An error is issued if a **set fields** operation sets a field on related objects but no related objects exist. A solution for this is to include a condition that confirms that at least one related object exists. For example, include a condition that confirms that a required field, such as Name, is not empty. Such a condition returns false if no related objects exist and, therefore, prevents the operation from being executed.

Procedure

1. In the GRC Workflow Designer, click the action that you want to edit.
The **Action Properties** panel opens.
2. Expand **Validations and Operations**.
3. Click **New Operation**. The **Operations** panel opens.
4. Set **Operation to set fields**.
5. Provide a **Name** for the operation.
6. Next to **When**, click **New Condition** to define one or more conditions. The **When** panel opens.

All conditions must be met for the operation to complete. For each condition you build a comparison statement with two fields and an operator.

- a) In **Compare**, you define the first field in the comparison statement. You can choose:
 - **A field in the current object**
Select an **Object Field**.
 - **A field in a related object**
 - Select Direct Child, Direct Parent, Ancestor, or Descendant in **Relationship Type**.
 - Select an object type in **Related Object Type**.
 - Select a field in **Related Object Field**.
 - Select a path in **Relationship Paths** (displays only if **Relationship Type** is Ancestor or Descendant).
 - Add **Filter By** conditions (optional).

- Set **Primary Parent Only** (displays only if **Relationship Type** is Direct Parent or Ancestor) (optional).

- **A field in a Preference object**

Select a **Preference Object Field**. You can add **Filter By** conditions.

- **End User**

An **End User** condition checks whether the signed on end user is a specified user and whether the user is in a specified user group. The second field in the comparison statement is a specified value, an expression, or an actor field on an object.

- b) In **Using**, choose an **Operator**. The list of operators depends on the field type of the field you chose in **Compare**.

- c) In **To**, you define the second field in the comparison statement. You can choose:

- **A specified value**

The value that you can provide depends on the field type of the field you chose in **Compare**. The comparison is case sensitive, so ensure that you specify the correct case for the value.

- **An expression**

Enter a single field or variable from the list in “[Using variables, functions, and fields](#)” on page 377. All of the variables and fields listed there can be used in an expression. The field or variable must be in the given format. It can, however, be part of a longer string, for example, a file name like Evidence_[**\$Parent:SOXRisk/System Fields:Name\$**].pdf if you want to validate that the parent object has a specific PDF attachment.

- **A field in the current object**

Select an **Object Field**.

- **A field in a related object**

- Select **Direct Child**, **Direct Parent**, **Ancestor**, or **Descendant** in **Relationship Type**.
- Select an object type in **Related Object Type**.
- Select a field in **Related Object Field**.
- Select a path in **Relationship Paths** (displays only if **Relationship Type** is Ancestor or Descendant).
- Add **Filter By** conditions (optional).
- Set **Primary Parent Only** (displays only if **Relationship Type** is Direct Parent or Ancestor) (optional).

- **A field in a Preference object**

Select a **Preference Object Field**. You can add **Filter By** conditions.

- d) If you chose a date field in **Compare**, you can define an offset in **Adjust Date By**.

- **A specified value** and enter **Number of Days**.

- **A field in the current object**

- **A field in a related object**

- Select Direct Child, Direct Parent, Ancestor, or Descendant in **Relationship Type**.
- Select an object type in **Related Object Type**.
- Select a field in **Related Object Field**.
- Select a path in **Relationship Paths** (displays only if **Relationship Type** is Ancestor or Descendant).
- Add **Filter By** conditions (optional).
- Set **Primary Parent Only** (displays only if **Relationship Type** is Direct Parent or Ancestor) (optional).

- **A field in the Preference object**

You can add **Filter By** conditions.

e) Click **Done**.

The condition is saved and assigned a number. Conditions are numbered consecutively in the order they are defined.

f) Optional: Add more conditions.

g) Optional: Set **Advanced Logic** to true to override the default rule that all conditions must be met.

Write a statement in **Logic**. Use the condition numbers together with the operators and, or, not, and parentheses.

The order of operations is: () then NOT then AND then OR.

For example:

- 1 or 2 or 3
- 1 and (2 or 3)
- 1 not (2 or 3)

7. Set **Execute As System** to **False** to execute the action as the logged in user. Set **Execute As System** to **True** to execute the action as the OPSystem user. The action can then perform operations that the logged in user cannot. The history on the **Activity** tab shows OPSystem as the user who performed the action.

When you set **Execute As System** to **True**, all set field operations where **Target Objects** is set to **Self** are also executed as the OPSystem user.

8. Click **Edit** next to **Target Objects**. Define what objects contain the fields that will be set.

a. Select a **Relationship Type**:

- Self
- Direct Child
- Direct Parent
- Ancestor
- Descendant

b. Select a **Related Object Type**. The list is filtered based on what you chose in **Relationship Type**.

c. Click **New Condition** to add a condition for setting the field on the target object.

d. If you chose Ancestor or Descendant in **Relationship Type**, select a path in **Relationship Paths**.

e. Click **Done**.

9. Add **Fields** and set their values on the selected object.

10. Click **Done**.

Defining a workflow action that starts a workflow

A **start workflow** operation on an action launches a workflow for a related object.

Before you begin

Define a workflow and add stages and actions to it. For information about how to define an action, “[Defining a workflow action](#)” on page 407.

Procedure

1. In the GRC Workflow Designer, click the action that you want to edit.

The **Action Properties** panel opens.

2. Expand **Validations and Operations**.

3. Click **New Operation**. The **Operations** panel opens.

4. Set **Operation** to **start a workflow**.

5. Provide a **Name** for the operation.

6. Next to **When**, click **New Condition** to define one or more conditions. The **When** panel opens.

All conditions must be met for the operation to complete. For each condition you build a comparison statement with two fields and an operator.

a) In **Compare**, you define the first field in the comparison statement. You can choose:

- **A field in the current object**

Select an **Object Field**.

- **A field in a related object**

– Select Direct Child, Direct Parent, Ancestor, or Descendant in **Relationship Type**.

– Select an object type in **Related Object Type**.

– Select a field in **Related Object Field**.

– Select a path in **Relationship Paths** (displays only if **Relationship Type** is Ancestor or Descendant).

– Add **Filter By** conditions (optional).

– Set **Primary Parent Only** (displays only if **Relationship Type** is Direct Parent or Ancestor) (optional).

- **A field in a Preference object**

Select a **Preference Object Field**. You can add **Filter By** conditions.

- **End User**

An **End User** condition checks whether the signed on end user is a specified user and whether the user is in a specified user group. The second field in the comparison statement is a specified value, an expression, or an actor field on an object.

b) In **Using**, choose an **Operator**. The list of operators depends on the field type of the field you chose in **Compare**.

c) In **To**, you define the second field in the comparison statement. You can choose:

- **A specified value**

The value that you can provide depends on the field type of the field you chose in **Compare**. The comparison is case sensitive, so ensure that you specify the correct case for the value.

- **An expression**

Enter a single field or variable from the list in “[Using variables, functions, and fields](#)” on page 377. All of the variables and fields listed there can be used in an expression. The field or variable must be in the given format. It can, however, be part of a longer string, for example, a file name like Evidence_[\\$Parent:SOXRisk/System Fields:Name\$].pdf if you want to validate that the parent object has a specific PDF attachment.

- **A field in the current object**

Select an **Object Field**.

- **A field in a related object**

– Select **Direct Child, Direct Parent, Ancestor, or Descendant** in **Relationship Type**.

– Select an object type in **Related Object Type**.

– Select a field in **Related Object Field**.

– Select a path in **Relationship Paths** (displays only if **Relationship Type** is Ancestor or Descendant).

– Add **Filter By** conditions (optional).

- Set **Primary Parent Only** (displays only if **Relationship Type** is Direct Parent or Ancestor) (optional).
- **A field in a Preference object**

Select a **Preference Object Field**. You can add **Filter By** conditions.

- d) If you chose a date field in **Compare**, you can define an offset in **Adjust Date By**.

- **A specified value** and enter **Number of Days**.
- **A field in the current object**
- **A field in a related object**
 - Select Direct Child, Direct Parent, Ancestor, or Descendant in **Relationship Type**.
 - Select an object type in **Related Object Type**.
 - Select a field in **Related Object Field**.
 - Select a path in **Relationship Paths** (displays only if **Relationship Type** is Ancestor or Descendant).
 - Add **Filter By** conditions (optional).
 - Set **Primary Parent Only** (displays only if **Relationship Type** is Direct Parent or Ancestor) (optional).

- **A field in the Preference object**

You can add **Filter By** conditions.

- e) Click **Done**.

The condition is saved and assigned a number. Conditions are numbered consecutively in the order they are defined.

- f) Optional: Add more conditions.

- g) Optional: Set **Advanced Logic** to true to override the default rule that all conditions must be met. Write a statement in **Logic**. Use the condition numbers together with the operators and, or, not, and parentheses.

The order of operations is: () then NOT then AND then OR.

For example:

- 1 or 2 or 3
- 1 and (2 or 3)
- 1 not (2 or 3)

7. Set **Execute As System** to **False** to execute the action as the logged in user. Set **Execute As System** to **True** to execute the action as the OPSSystem user. The action can then perform operations that the logged in user cannot. The history on the **Activity** tab shows OPSSystem as the user who performed the action.

When you set **Execute As System** to **True**, all set field operations where **Target Objects** is set to **Self** are also executed as the OPSSystem user.

8. Click **Edit** next to **Target Objects** to define the object that the workflow is started for.

- a. Select a **Relationship Type**:

- Direct Child
- Direct Parent
- Ancestor
- Descendant

- b. Select a **Related Object Type**. The list is filtered based on what you chose in **Relationship Type**.

- c. Click **New Condition** next to **Filter By** to add a condition to the target object.

- d. If you chose Ancestor or Descendant in **Relationship Type**, select a path in **Relationship Paths**.

9. In **Workflow** enter the name of the workflow to start. The workflow must be for object type designated in **Related Object Type** and it must be published.

10. Click **Done**.

Results

When the action takes place, the new workflow starts. Both workflows continue and are independent of each other.

Defining a workflow action that runs a calculation

A **run a calculation** operation on an action runs a calculation on an object.

Before you begin

Define a workflow and add stages and actions to it. For information about how to define an action, [“Defining a workflow action” on page 407](#).

Define and publish the calculation that the action runs. The calculation type must be manual. For more information, see [“Defining a calculation” on page 338](#).

Procedure

1. In the GRC Workflow Designer, click the action that you want to edit.

The **Action Properties** panel opens.

2. Expand **Validations and Operations**.

3. Click **New Operation**. The **Operations** panel opens.

4. Set **Operation** to **run a calculation**.

5. Provide a **Name** for the operation.

6. Next to **When**, click **New Condition** to define one or more conditions. The **When** panel opens.

All conditions must be met for the operation to complete. For each condition you build a comparison statement with two fields and an operator.

a) In **Compare**, you define the first field in the comparison statement. You can choose:

- **A field in the current object**

Select an **Object Field**.

- **A field in a related object**

– Select Direct Child, Direct Parent, Ancestor, or Descendant in **Relationship Type**.

– Select an object type in **Related Object Type**.

– Select a field in **Related Object Field**.

– Select a path in **Relationship Paths** (displays only if **Relationship Type** is Ancestor or Descendant).

– Add **Filter By** conditions (optional).

– Set **Primary Parent Only** (displays only if **Relationship Type** is Direct Parent or Ancestor) (optional).

- **A field in a Preference object**

Select a **Preference Object Field**. You can add **Filter By** conditions.

- **End User**

An **End User** condition checks whether the signed on end user is a specified user and whether the user is in a specified user group. The second field in the comparison statement is a specified value, an expression, or an actor field on an object.

b) In **Using**, choose an **Operator**. The list of operators depends on the field type of the field you chose in **Compare**.

c) In **To**, you define the second field in the comparison statement. You can choose:

- **A specified value**

The value that you can provide depends on the field type of the field you chose in **Compare**. The comparison is case sensitive, so ensure that you specify the correct case for the value.

- **An expression**

Enter a single field or variable from the list in “[Using variables, functions, and fields](#)” on page 377. All of the variables and fields listed there can be used in an expression. The field or variable must be in the given format. It can, however, be part of a longer string, for example, a file name like Evidence_[**\$Parent:SOXRisk/System Fields:Name\$**].pdf if you want to validate that the parent object has a specific PDF attachment.

- **A field in the current object**

Select an **Object Field**.

- **A field in a related object**

- Select **Direct Child**, **Direct Parent**, **Ancestor**, or **Descendant** in **Relationship Type**.
- Select an object type in **Related Object Type**.
- Select a field in **Related Object Field**.
- Select a path in **Relationship Paths** (displays only if **Relationship Type** is Ancestor or Descendant).
- Add **Filter By** conditions (optional).
- Set **Primary Parent Only** (displays only if **Relationship Type** is Direct Parent or Ancestor) (optional).

- **A field in a Preference object**

Select a **Preference Object Field**. You can add **Filter By** conditions.

d) If you chose a date field in **Compare**, you can define an offset in **Adjust Date By**.

- **A specified value** and enter **Number of Days**.

- **A field in the current object**

- **A field in a related object**

- Select **Direct Child**, **Direct Parent**, **Ancestor**, or **Descendant** in **Relationship Type**.
- Select an object type in **Related Object Type**.
- Select a field in **Related Object Field**.
- Select a path in **Relationship Paths** (displays only if **Relationship Type** is Ancestor or Descendant).
- Add **Filter By** conditions (optional).
- Set **Primary Parent Only** (displays only if **Relationship Type** is Direct Parent or Ancestor) (optional).

- **A field in the Preference object**

You can add **Filter By** conditions.

e) Click **Done**.

The condition is saved and assigned a number. Conditions are numbered consecutively in the order they are defined.

f) Optional: Add more conditions.

g) Optional: Set **Advanced Logic** to true to override the default rule that all conditions must be met.

Write a statement in **Logic**. Use the condition numbers together with the operators and, or, not, and parentheses.

The order of operations is: () then NOT then AND then OR.

For example:

- 1 or 2 or 3
- 1 and (2 or 3)
- 1 not (2 or 3)

7. Set **Execute As System** to **False** to execute the action as the logged in user. Set **Execute As System** to **True** to execute the action as the OPSystem user. The action can then perform operations that the logged in user cannot. The history on the **Activity** tab shows OPSystem as the user who performed the action.

When you set **Execute As System** to **True**, all set field operations where **Target Objects** is set to **Self** are also executed as the OPSystem user.

8. Click **Edit** next to **Target Objects** to define the object that the workflow is started for.

a. Select a **Relationship Type**:

- Self
- Direct Child
- Direct Parent
- Ancestor
- Descendant

b. Select a **Related Object Type**. The list is filtered based on what you chose in **Relationship Type**.

c. Click **New Condition** next to **Filter By** to add a condition to the target object.

d. If you chose Ancestor or Descendant in **Relationship Type**, select a path in **Relationship Paths**.

9. In **Calculation** enter the name of the calculation to start. The calculation must be for the same object type as the workflow, it must be published, and the calculation type must be manual.

10. Click **Done**.

Deleting actions

In the GRC Workflow Designer, you can delete actions.

Procedure

To delete an action from a workflow, choose one of the following options:

- Select an action on the canvas and press Delete on the keyboard.
- Select an action on the canvas and click **Delete Action** in the action property panel.

Customizing email notification templates in workflows

You can customize email notifications for end stages and any action that doesn't end with an end stage.

About this task

Procedure

1. Click  > **Solution Configuration** > **Workflows**.
2. Click the workflow that you want to edit.
The GRC Workflow Designer opens.
3. On the canvas, select the action or end stage for which you want to customize the email notification templates.

For actions, use the following steps:

4. In the **Action properties** panel, expand the **Email** section, and set the following options to **True** to send email notifications when the action completes:

- **Notify Assignees**

When you set **Notify Assignees** to **True**, the **Customize** link is displayed so that you can customize the assignee subject and body templates for email notifications.

- **Notify Subscribers**

When you set **Notify Subscribers** to **True**, the **Customize** link is displayed so that you can customize the subscriber subject and body templates for email notifications.

5. To customize email notifications for subscribers or assignees, click **Customize**. For the subject and body of the email, choose one of the following steps:

- a. Select a template from the list of templates and edit the string. Any changes made to the string apply to any email notification that uses the string.

- b. Click **Copy to new template**, enter a template name, and click **Copy**.

Edit the text for the new template.

6. To translate the templates, click **Translations** and do one of the following steps:

- Enter the translation of the application text for each language.

- If it is displayed, click  to populate translated application text for each language. For more information, see “IBM Watson Language Translator” on page 847.

7. To preview the email message, click **Preview**.

8. Click **Done**.

For an end stage, use the following steps:

9. In the **Stage properties** panel, expand the **End Stage Notifications** section, and click **Customize email template**.

10. For the subject and body of the email, choose one of the following steps:

- a. Select a template from the list of templates and edit the string. Any changes made to the string apply to any email notification that uses the string.

- b. Click **Copy to new template**, enter a template name, and click **Copy**.

Edit the text for the new template.

11. To translate the templates, click **Translations** and do one of the following steps:

- Enter the translation of the application text for each language.

- If it is displayed, click  to populate translated application text for each language. For more information, see “IBM Watson Language Translator” on page 847.

12. To preview the email message, click **Preview**.

13. Click **Done**.

Results

Changes to text in an existing email template or new email templates that are created in the Workflow Designer can be seen on the Application Text screen, and any edits that are performed on the Application Text screen can be seen in the Workflow Designer. The name of the template you see in the Workflow Designer is prefixed with **com.wf.email.template**. for the corresponding name on the Application Text screen. For more information about editing application text, see [Modifying application text](#).

Creating objects based on scores in a questionnaire assessment

You can configure the Questionnaire Assessment Workflow to create an object, such as an issue, when the score for the response to a question doesn't meet a set threshold.

Any files that are attached to the answered question are automatically attached to the created object.

You can create any object type except for Files (SOXDocument) and Links (SOXExternalDocument).

For more information about how scores are calculated, see *Questionnaires* in the *IBM OpenPages with Watson User Guide*.

About this task

To perform this task, you must be an administrator with the application permission **SOX > Administration > Workflow**.

Procedure

1. To open the GRC Workflow Designer, click  > **Solution Configuration** > **Workflows**.
2. Click **Questionnaire Assessment Workflow**.
3. Select an action between two stages. For example, for a two stage questionnaire assessment, you can select the action **Submit and Close** between the **Information Gathering** stage and the **Closed** stage.
The **Action Properties** panel appears.
4. Expand the **Validations and Operations** section.
5. Click **New Operation**.
6. In the **Operation** field, select **Custom action**.
7. Enter a **Name**.
8. In the **Class Name** field, enter
com.ibm.openpages.api.service.local.workflow.actions.QuestionnaireScoreAssessmentAction.
9. Set the threshold:
 - a) Click **Add Property**.
 - b) Enter the **Name** of the property, **threshold**, and a **Value**, such as **4**. When you set the value to **4**, an object, such as an issue, is generated when a score for an answer is less than 4. If you don't specify the property **objectType** in step 10, an issue is generated by default.
The default value of the **threshold** property is **5**.
 - c) In the **Properties** panel, click **Done**.
10. Optional: If you want to create an object type other than an issue (the default), set the object type:
 - a) Click **Add Property**.
 - b) Enter the **Name** of the property, **objectType**, and a **Value**, such as **SOXRisk**. When you set the value to **SOXRisk**, a risk is generated when a score for an answer is less than the set threshold.
The default value of the **objectType** property is **SOXIssue**.
The **objectType** property must specify the system name, such as **SOXRisk**, rather than the display name, such as **Risk**. The object type must be a child of the asset type.
 - c) In the **Properties** panel, click **Done**.
11. In the **Operations** panel, click **Done** and click **Publish**.

Results

When the questionnaire assessment triggers the custom action, the questionnaire assessment shows an icon to point out each answer that has a score below the set threshold and an object, such as an issue, is created.

In the following example, an issue is created because the **objectType** property was not specified.

The screenshot shows a questionnaire interface. At the top, it says "Questionnaire". Below that, "Section 1/1". Under "Section 1/1", there's a "SubSection 1/1" panel. Inside this panel, there's a section titled "1.1.1. Example" with a "default description *". Below this, there's a dropdown menu with three options: "Low score" (selected), "No", and "Not applicable". To the right of the dropdown, there are icons for edit, delete, and save, followed by "Weight: 1" and "Score: 2".

Figure 59. A section of a questionnaire showing the low score icon

The following figure shows the **Parent and child relationships** diagram for a questionnaire assessment. The relationships are expanded to show an issue as a child of the resource.

Parent and child relationships

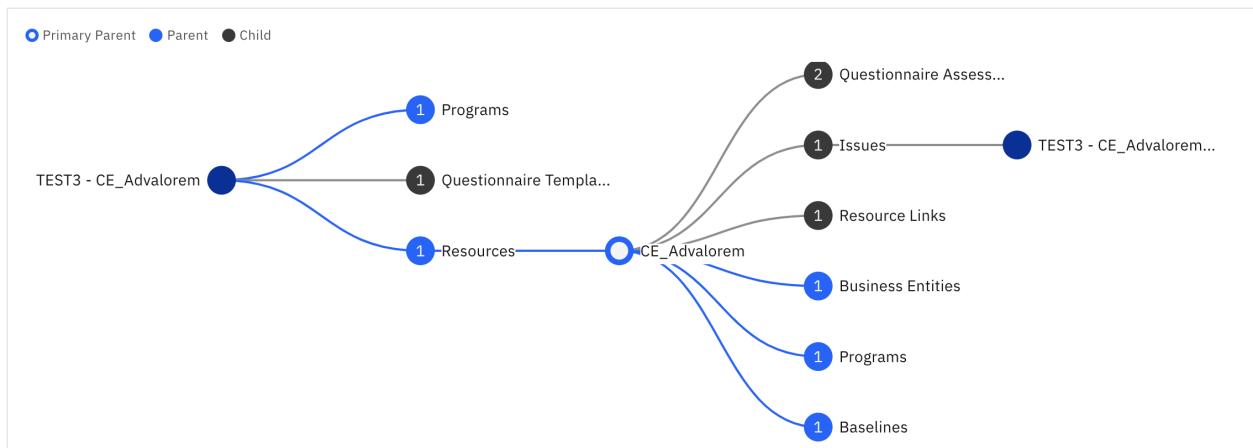


Figure 60. Parent and child relationship diagram showing an issue

Starting workflow instances in bulk

As an administrator, you can start a single workflow that creates workflow instances in bulk. A workflow instance starts for each object that meets the start conditions.

Before you begin

Verify that email notifications for a bulk process are configured. For more information, see “[Customizing email notifications for GRC Workflow](#)” on page 432.

Plan when you run the bulk update. Depending on how many workflow instances are started, the bulk process can take a long time and may affect system performance for other users.

About this task

You can run a bulk process for one workflow at a time.

Procedure

1. Click  > **Solution Configuration > Workflows**.
2. From the Workflow List, select a single workflow with a check mark.
Start Workflow displays as one of the bulk update options.
3. Click **Start Workflow**.
A message provides an estimated count of the affected objects.
4. Click **Start Workflow**.
A workflow instance starts for each object of the workflow's object type if all of the following conditions are met:
 - The workflow is published.
 - The workflow is enabled.
 - An object is not locked.
 - An object is not currently in another workflow process.
 - An object meets the workflow's applicability criteria.
 - Your user is allowed to start a workflow for an object, given the conditions and applicability defined in the workflow. For all workflow instances that are started, your user is saved in the System Workflow Fields:Workflow Start User field.
5. When the process finishes, go to  > **Other > Background Processes** and review the log.
You receive an email that summarizes the bulk process. The assignees and subscribers of the workflow also receive email notifications.

Managing workflow instances

Monitor workflow instances to ensure that they are completing in a timely manner. Terminate stopped or blocked workflow instances.

Procedure

1. Click  > **Solution Configuration > Workflows**.
2. Click **Workflow Instances**.
A list of active workflow instances is displayed.
3. Filter the list of workflow instances by:
 - **Criticality**
 - **Workflow name**
 - **Stage**
 - **Type** (object type)
4. You can sort the list by fields in the header row.
5. You can click a workflow instance to open it.
6. To terminate a workflow instance, select it and click **Terminate Workflow Instances**.
The workflow instance is deleted. The object the workflow was based on remains but the workflow information, for example, workflow name, stage, and assignee, is removed. You can restart the workflow for the same object if needed.

Exporting and importing workflow definitions

You can migrate workflow definitions from one environment to another environment using Export Configuration and Import Configuration.

Before you begin

Read Chapter 26, “[Migrating OpenPages environments](#),” on page 719 to ensure that you are familiar with how to use Export Configuration and Import Configuration.

About this task

When you export workflows using Export Configuration, the workflow definitions you select are exported to a migration file. The email templates referenced in the exported workflow files are also automatically exported. Task Views and object types that are referenced in the workflows are not exported.

Procedure

1. Follow the instructions described in [“Exporting and importing workflow definitions” on page 432](#) and choose the workflows to export.
2. Follow the instructions described in [“Importing a migration file ” on page 729](#) to import the migration file into a target environment.
3. Access and test the workflows in the target environment. Verify that the Task Views and object types work with the Task Views you migrated.

Customizing email notifications for GRC Workflow

You can customize the content of the email notifications that are generated by GRC Workflow by defining application text that is specific to your organization.

Before you begin

Learn about the **Email** setting on workflow actions. For information, see [“Defining a workflow action” on page 407](#).

Learn about the **End Stage Notifications** setting on workflow end stages. For information, see [“Defining an end stage” on page 402](#).

Learn about starting workflow instances in bulk. For information, see [“Starting workflow instances in bulk” on page 430](#). At the end of a bulk update process, a summary email notification is sent to the administrator who started the process and email notifications are sent to assignees and subscribers.

Ensure that registry settings that apply to email notifications have been defined. For information, see [“Setting up GRC Workflow” on page 369](#).

About this task

You can use the default email template as-is or customize the text to meet your requirements. There is one email template for all workflows and all object types. It is used for email notifications that are sent to users and summary email notifications that are sent to administrators who start a bulk update. The text and fields must be appropriate for broad use. You cannot create a new template.

If you operate in multiple locales, you can define email content in different languages. The template is designed for multiple formats, including tablets and phones.

If you customize the text, you define the content of the email notifications using application text strings. The email subject content is plain text. The email body content is formatted in HTML. You can apply styles using embedded style sheets.

You can also insert variables and fields in the email body content. For more information, see [“Using variables, functions, and fields ” on page 377](#). All the variables and fields that are listed there can be inserted in the email body content. Since there is only one email template for all workflows, insert system

workflow fields rather than object fields. For more information, see “[System workflow fields](#)” on page 376.

Example:

```
<!DOCTYPE HTML>
<html>
  <head></head>
  <body style="font-family: ibm-plex-sans,HelveticaNeue,Helvetica,Arial,sans-serif; font-size: 14px;">
    <h1 style="font-size: 20px; font-weight: 300; padding: 22px 24px;">IBM <span style="font-weight: 600">OpenPages with Watson</span></h1>
    <hr style="margin: 0; border-bottom: 2px solid #009e9a;">
    <div style="padding: 8px 24px 32px; background-color: #f3f3f3;">
      <h2 style="font-size: 14px; font-weight: 600; margin: 24px 0 8px;">[$System Fields:Object Type Label$]:</h2>
      <p style="margin: 0;"><a href="#">[$System Fields:Task View URL$]>[$System Fields:Name$]</a></p>
      <h2 style="margin: 0; display: none[$DaysFromNow/System Workflow Fields:Stage Due Date$];">Due in [$DaysFromNow/System Workflow
Fields:Stage Due Date$] days ([$System Workflow Fields:Stage Due Date$])</h2>
      <p style="margin: 0;">[$ApplicationText/app.workflow.workflowInfo.duedate.label$]:</h2>
      <h2 style="font-size: 14px; font-weight: 600; margin: 24px 0 8px;">[$ApplicationText/app.workflow.workflowInfo.criticality.label$]:</h2>
      <p style="margin: 0;">[$System Workflow Fields:Workflow Criticality$]</p>
    </div>
    <div style="padding: 8px 24px 160px;">
      <h2 style="font-size: 14px; font-weight: 600; margin: 24px 0 8px;">[$ObjectText/System Fields:Description$]:</h2>
      <p style="margin: 0;">[$System Fields:Description$]</p>
      <h2 style="font-size: 14px; font-weight: 600; margin: 24px 0 8px;">[$ApplicationText/app.workflow.workflowInfo.stage.label$]:</h2>
      <p style="margin: 0;">[$System Workflow Fields:Stage Name$]</p>
      <h2 style="font-size: 14px; font-weight: 600; margin: 24px 0 8px;">[$ApplicationText/app.workflow.transition.status$]:</h2>
      <p style="margin: 0;">[$System Workflow Fields:Workflow Status$]</p>
    </div>
    <hr style="margin: 0; border-bottom: 1px solid #767676;">
    <div style="padding: 32px 24px;">This email was automatically generated by [$ApplicationText/product.name$].</div>
  </body>
</html>
```

Procedure

1. Click  **System Configuration > Application Text**.
2. Click  to access the search filter.
3. Click **Email Templates**.
4. Use **Search** to further refine the list.
5. Select the application text you want to modify:
 - `com.wf.email.template.default.assignee.subject` contains the text in the subject line of emails sent to assignees.
 - `com.wf.email.template.default.assignee.body` contains the text in the body of emails sent to assignees.
 - `com.wf.email.template.default.subscriber.subject` contains the text in the subject line of emails sent to subscribers.
 - `com.wf.email.template.default.subscriber.body` contains the text in the body of emails sent to subscribers.
 - `com.wf.email.template.default.action.complete.subject` contains the text in the subject of emails for long running processes. This email informs the user that the process has finished. It is sent to the person who started the action.
 - `com.wf.email.template.default.action.complete.body` contains the text in the body of emails for long running processes. This email informs the user that the process has finished. It is sent to the person who started the action.
 - `com.wf.email.template.bulk.start.subject` contains the subject line of emails for Start Workflows bulk update (long running processes). This email informs the user that the process has finished. It is sent to the person who started the action.
 - `com.wf.email.template.bulk.start.body` contains the text in the body of emails for Start Workflows bulk update (long running processes). This email informs the user that the process has finished. It is sent to the person who started the action.
 - `com.wf.email.template.bulk.start.failure.part` contains the failure text in the body of emails Start Workflows bulk update (long running processes). This email informs the user about failures. It is sent to the person who started the action.
6. For each locale, enter the content that you want to appear in the email notification.

If it is displayed, click  to populate translated values to languages. For more information, see “[IBM Watson Language Translator](#)” on page 847.

7. Click **Done**.

Reporting on information in workflow instances

You can write reports that include information from workflow fields on workflow instances.

Before you begin

- Define the Include Workflow Fields setting as true. For more information, see [“Including workflow fields” on page 807](#).
- Regenerate the reporting framework to make workflow instance data available to report authors.

About this task

All object types have workflow fields. Report authors can include those fields in reports. For more information, see [“System workflow fields” on page 376](#).

The full set of information is available in DQM Standard framework models, while a subset is available in Basic framework models. The information is available in workflow-specific query subjects and a subset of the information is available on every object type in the framework.

Chapter 17. Scheduler

Use the Scheduler to define and manage jobs that are run manually or on a schedule. The Scheduler is also used to view job executions that have completed.

Managing jobs

Use the Scheduler to manage jobs.

To access the Scheduler, click  > **Solution Configuration** > **Scheduler**. Whether the menu item is displayed depends on your access permissions.

Kinds of jobs

The Scheduler is used to manage the following kinds of jobs:

- Custom jobs

Custom jobs are user-defined jobs that perform a function. These jobs are configured, edited, viewed, manually started, and deleted in the Scheduler. For more information, see “[Defining a custom job](#)” on page 437.

- JSP report jobs

A JSP report job is a custom job that runs a JSP report. These jobs are configured, edited, viewed, manually started, and deleted in the Scheduler. For more information, see “[Defining a job that runs a JSP report](#)” on page 438.

- Workflow Start jobs

Workflow Start jobs are created automatically in the Scheduler for workflows that are defined with a scheduled start. They can be viewed and manually started in the Scheduler. You can edit the description of the job but the schedule cannot be changed in the Scheduler. For more information, see “[Defining a workflow](#)” on page 391.

- Ascent job

The Ascent job is displayed automatically in the Scheduler if the Ascent feed is used. The job defines the configuration and scheduling for the Ascent feed. You can view, edit, and start the job manually. For more information, see “[Ascent Connector](#)” on page 893.

- Reg-Track job

This job is displayed automatically in the Scheduler when you run a Reg-Track import. For more information, see “[Reg-Track connector](#)” on page 901.

- RapidRatings job

This job is displayed automatically in the Scheduler if the RapidRatings connector is installed. For more information, see “[RapidRatings connector for IBM OpenPages Third Party Risk Management](#)” on page 921.

- RiskLens job

This job is displayed automatically in the Scheduler if the RiskLens connector is installed. For more information, see Chapter 35, “[IBM OpenPages IT Governance with RiskLens](#),” on page 881.

- RiskRecon job

This job is displayed automatically in the Scheduler if the RiskRecon connector is installed. For more information, see “[RiskRecon connector for IBM OpenPages Third Party Risk Management](#)” on page 922.

- SecurityScorecard job

The SecurityScorecard job is displayed automatically in the Scheduler if the SecurityScorecard feed is used. The job defines the configuration and scheduling for the SecurityScorecard feed. You can view, edit, and start the job manually. For more information, see “[SecurityScorecard connector for IBM OpenPages Third Party Risk Management](#)” on page 919.

- SupplyWisdom job

The SupplyWisdom job is displayed automatically in the Scheduler if the SupplyWisdom feed is used. The job defines the configuration and scheduling for the SupplyWisdom feed. You can view, edit, and start the job manually. For more information, see “[Supply Wisdom connector](#)” on page 920.

- Thomson Reuters Regulatory Intelligence job

This job is displayed automatically in the Scheduler when you run a Thomson Reuters Regulatory Intelligence import. For more information, see “[Thomson Reuters Connector](#)” on page 895.

- Wolters Kluwer job

This job is displayed automatically in the Scheduler when you run a Wolters Kluwer import. For more information, see “[Wolters Kluwer Connector](#)” on page 906.

Schedule List

When you click  > **Solution Configuration** > **Scheduler**, a Schedule List is displayed.

From the Schedule List, you can:

- Select the check box next to single or multiple jobs and click **Start Job**  to manually start a job. You might want to start a job manually if you do not want to wait for the next scheduled time or if the job has no schedule.

The Start Job Report window displays the number of jobs that started and failed.

- Click a job name. Information about the job opens in a new tab. Select the **Executions** tab to view information about each job execution.
- Click the **Job Name** column header to change the sort order of the list.
- Select the check box next to single or multiple jobs. The bulk update options are:
 - Enable
 - Disable
 - Delete
 - Start Job
- Click  to filter the Schedule List by category, such as Workflow Start, Custom, and so on.

Create a new custom job

Click **New Job** to create a new job. For more information, see “[Defining a custom job](#)” on page 437.

Delete a custom job

To delete a custom job, select a job from the Schedule List and click **Delete**. Non-custom jobs, for example, Workflow Start, cannot be deleted in the Scheduler.

Disable a job

To disable a job, select a job from the Schedule List. Select **Disable**.

Set timeouts for jobs

The default timeout for all scheduler jobs is defined in the **Platform** > **Scheduler** > > **Default Transaction Timeout** setting. The default value is 3600 seconds.

Custom jobs can have custom timeout settings that override the **Default Transaction Timeout**. The timeout settings for custom jobs are defined in **Platform > Processes > <Custom_job_name> > Transaction timeout**. The `<Custom_job_name>` is the name that is defined in the constructor by using the `super.setName("your job name");` method. For more information, see “[Implementing a Java class for custom jobs](#)” on page 440.

Defining a custom job

A custom job definition contains information about a job and when it is executed.

Before you begin

Implement the Java class. For more information, see “[Implementing a Java class for custom jobs](#)” on page 440.

About this task

A custom job is typically defined with a schedule so that it runs, for example, every night at midnight. But a custom job can also be defined without a schedule. A custom job, like all jobs, can be started manually at any time.

Procedure

1. Click  > **Solution Configuration** > **Scheduler**.
2. Click **New Job**.
The **New Job** panel opens.
3. Enter an internal **Name** for the custom job. It cannot be changed later.
Allowed characters are A-Z, a-z, 0-9, underscore, hyphen, and spaces. Special characters are not allowed.
4. Enter a **Description**.
5. Enter a **Java class name** of the class that you created as a prerequisite.
6. Leave **Enabled** selected. It can be changed later.
7. In **Custom configuration** click **Add** to define properties that are name-value pairs needed by the Java class.
 - a) Enter a **Name**.
 - b) Set **Encrypt** to true or false.
 - c) Enter a **Value**.
8. Click **Edit** next to **Schedule** to set up a repeatable schedule. Otherwise, leave **Schedule** set to Not scheduled.
 - a) Enter a **Name**.
The **Name** displays in the Scheduler as the **Schedule Name**. Allowed characters are A-Z, a-z, 0-9, underscore, hyphen, and spaces. Special characters are not allowed.
 - b) Enter a **Description** (optional).
 - c) Select a schedule type in **Define Schedule**:
 - Recurring
 - Specified Date/Time
 - Cron Expression
 - d) If you chose Recurring:
 - Select a value in **Repeat** (Daily, Weekly, Monthly, Quarterly) and add details such as day, month, or quarter.

- Enter a **Time of Day**.
 - Select an **End Date** (optional).
- e) If you chose Specified Date/Time:
- Select a **Date**.
 - Enter a **Time of Day**.
- f) If you chose Cron Expression:
- Enter a **Cron Expression**.
 - Select an **End Date** (optional).
- Advanced users can choose a cron expression if a Recurring or Specified Date/Time schedule does not meet your needs. Use the syntax for cron expressions, not crontab expressions.
- g) Click **Done**.
9. Click **Done**.

Defining a job that runs a JSP report

You can use the Scheduler to create jobs that automatically run JSP reports.

Before you begin

- To do this task, you need the **Scheduler** application permission.
- You need a JSP report. For more information, see [“Creating an interactive JSP report” on page 139](#).

About this task

You run JSP report jobs by using a custom job, which is available by default. You specify the JSP report to run, parameters for the job, and when to run the job.

For example, you can create a job that runs the KRI Creation Utility each week. The KRI Creation Utility is a JSP report that identifies KRIs that require values and sends notification emails to the KRI owners. Each week, the job runs the utility and sends the notifications automatically.

If the JSP report takes parameters, such as the name of a business entity or a profile, you can pass those parameters to the job.

The following table shows the required and optional parameters for JSP report jobs.

Item	Description
Java class	com.ibm.openpages.api.service.local.scheduler.jobs.JSPReportJob
Required parameter	JSPReport – Specifies the path to the JSP report. For example: Reporting/Hidden Reports/ORM Custom Reports/KRI Creation Utility/KRI Creation Utility
Optional parameters	<ul style="list-style-type: none"> • OutputEntity – Specifies the full path to a Business Entity object. The report output is attached to the Business Entity that you specify. • SaveOutput (true false) -- Specifies whether the output of the report is saved. Default is false. <p>If SaveOutput is true and OutputEntity is empty, the report output is saved to the /aurora/output/jspreport directory on the application server.</p>

Item	Description
	<ul style="list-style-type: none"> Report parameters – If the JSP report uses parameters, you can add the parameters to the job definition. Parameter names must match the report parameter names exactly. <p>If you add a parameter to the job definition, you must provide a value for the parameter. You cannot leave a parameter value empty.</p> <p>If the value of a parameter contains spaces, surround the value with quotation marks.</p>

Procedure

1. Log on as an administrator.
2. Collect the information that you need to run the JSP report:
 - a) Click  > **System Configuration** > **Pages and Templates**, locate the JSP report, and then click its name.
The report's details are displayed.
 - b) Get the report name and folder:
Copy the text in the **Folder** field. Remove / _cw_channels /, and then remove the spaces between each /. Add the report's name to the path.
For example: Reporting/Hidden Reports/ORM Custom Reports/KPI Creation Utility/KPI Creation Utility
 - c) If the JSP report uses parameters, get the parameter names. The parameter names are shown in the **Page Details** section.
 - d) If you want to attach the report output to a business entity, get the business entity's full path:
Click **Organization** > **Business Entities**, click the name of the business entity you want to use, and copy the value of the **Folder** field.
3. Click  > **Solution Configuration** > **Scheduler**.
4. Click **New Job**.
The **New Job** panel opens.
5. Enter a **Name** for the job. You can't change the name later.
Allowed characters are A-Z, a-z, 0-9, underscore, hyphen, and spaces. Special characters are not allowed.
6. Enter a **Description**.
7. In the **Java class name** field, paste the following text:


```
com.ibm.openpages.api.service.local.scheduler.jobs.JSPReportJob
```
8. Leave **Enabled** selected. You can change it later.
9. In **Custom configuration** click **New**.
10. In the **Name** field, type **JSPReport**. In the **Value** field, type the path the JSP report.
11. To define other parameters, click **New** and enter the parameter's name and value. Repeat this step for each parameter that you want to add.
12. Optional: To set up a repeatable schedule for the job, click **Edit** next to **Schedule** Otherwise, leave **Schedule** set to **Not scheduled**, and go to step 13.
 - a) Enter a **Name**.
The **Name** displays in the Scheduler as the **Schedule Name**. Allowed characters are A-Z, a-z, 0-9, underscore, hyphen, and spaces. Special characters are not allowed.
 - b) Enter a **Description** (optional).

c) Select a schedule type in **Define Schedule**:

- Recurring
- Specified Date/Time
- Cron Expression

d) If you chose Recurring:

- Select a value in **Repeat** (Daily, Weekly, Monthly, Quarterly) and add details such as day, month, or quarter.
- Enter a **Time of Day**.
- Select an **End Date** (optional).

e) If you chose Specified Date/Time:

- Select a **Date**.
- Enter a **Time of Day**.

f) If you chose Cron Expression:

- Enter a **Cron Expression**.
- Select an **End Date** (optional).

Advanced users can choose a cron expression if a Recurring or Specified Date/Time schedule does not meet your needs. Use the syntax for cron expressions, not crontab expressions.

g) Click **Done**.

13. Click **Create**.

Implementing a Java class for custom jobs

A custom job is a user-defined job that performs a function. It is implemented as a Java class that can be executed manually or on a schedule.

Custom jobs must be deployed to each OpenPages application server and are dynamically loaded during startup.

To implement a custom job, complete the following tasks:

- Create a custom job Java class by extending the following abstract implementation:

```
com.ibm.openapi.api.scheduler.AbstractScheduledProcess
```

- Add the class to a JAR file. Use the JAR file for all of your custom code. Deploy the JAR file to each OpenPages application server in the <OP_HOME>/aurora/op-ext-lib directory.
- Restart the OpenPages application servers so that the custom job can be picked up by the dynamic class loader.
- Use the Scheduler to add a custom job that uses the Java class. Set any property values or fields that the custom job requires as inputs. For more information, see [“Defining a custom job” on page 437](#).

Providing configuration information to a custom job

For a custom job to be useful, it might require configuration information. For example, if it needs to connect to another service, it may need to know the API key. These values are defined as configuration items in the custom job in the Scheduler and passed into the custom job at run time.

Configuration items are string name-value pairs that you define.

The custom job needs to validate that the properties that it expects to be passed in have been passed in and that they have valid values.

Authoring the custom job Java class

The only requirement of a custom job Java class is that it extends `com.ibm.openpages.api.scheduler.AbstractScheduledProcess`. This requirement is validated when the custom job is defined in the Scheduler.

Give the custom job a name. In the constructor of the job, make a call to `setName()`. For example, this code creates a custom job that is called My Custom Job:

```
public class CustomJob extends AbstractScheduledProcess {  
    public CustomJob() {  
        super(ProcessConstants.TYPE_GENERAL);  
        setName("My Custom Job");  
    }  
}
```

A single abstract API from `AbstractScheduledProcess` called `execute` must be implemented in your derived Java class. Within this method is where you write the functionality that the custom job performs.

```
void execute(){  
//add your custom code here  
}
```

To access the configuration values for the job, call:

```
this.jobDetail.getJobConfiguration();
```

For more information about the IBM OpenPages GRC Java API, which you can use in custom actions, see *IBM OpenPages GRC Java API* in the *IBM OpenPages with Watson Developer Guide*.

Exception or validation messages can be thrown from a custom job and displayed to the user. To display messages, use:

```
throwException(String message, Throwable cause)
```

Use this method to throw exceptions and display a custom message to users. Uncaught exceptions or exceptions that are explicitly thrown are logged by the application, but only a general error message is displayed to users.

Setting a timeout for the job

The default timeout for all scheduler jobs is defined in the **Platform > Scheduler > Default Transaction Timeout** setting. You can override this timeout setting for a custom job.

To set a timeout for a custom job, you need the custom job name, which is defined by `setName()` in the constructor of the job. Create the following setting to define the timeout: **Platform > Processes > <Custom_job_name> > Transaction timeout**.

For example: **Platform > Processes > My Custom Job > Transaction timeout**.

Chapter 18. Localizing text

You can localize display text for object types and fields, and for a variety of application objects and custom return values. You can manage localized text that displays to users for predefined object types, object fields that are supplied by IBM OpenPages with Watson or that you create, and application objects.

Locale codes

The OpenPages with Watson application provides translation support in several languages for predefined object text. Each supported language has a corresponding locale code that is listed under the object text. The locale code consists of a language code (for example, fr for French) and a country or region code (for example, FR for France).

The following table lists the supported languages with their corresponding locale code.

Table 146. Supported Languages and Locale Codes	
Language	Locale Code
German	de_DE
U.S. English	en_US
U.K. English	en_GB
Spanish	es_ES
French	fr_FR
Italian	it_IT
Japanese	ja_JP
Brazilian Portuguese	pt_BR
Simplified Chinese	zh_CN
Traditional Chinese	zh_TW
Report Design Language	en_CA
Note: Users authoring reports in the reporting tool must select this language prior to creating or modifying reports.	

The default language for object text that has not been translated is U.S. English.

You can globally set a default language in which the application user interface is displayed to users and optionally enable auditing of translation label changes. For details see “[Set localization options](#)” on page 503.

Configuring client systems to display Asian characters

You can install language packs on Microsoft Windows client machines to see Windows in other languages.

Note: For users who use the Japanese locale, client machines must have the Windows Japanese language pack installed. If this pack is not installed, IBM OpenPages with Watson users will notice that the browser title bar and some pop-up messages contain unreadable characters.

For more information, see [Language packs for Windows](#).

Language and locale support

If you are using IBM OpenPages with Watson in a language other than English, this information will help you to understand the language and locale settings.

Web browser language preference

The web browser language preference is the setting that you choose to specify the language that web pages can be displayed in. The web browser language preference affects only the OpenPages with Watson login page. The web browser language preference does not affect number and date formatting in OpenPages with Watson.

If the web browser language preference is set to a language other than one of the following languages, be aware that the OpenPages with Watson login page appears in English:

- German
- Spanish
- French
- Italian
- Japanese
- Portuguese
- Chinese
- English

Change Locale setting in OpenPages

Click  > **Change Locale** to see a list of product languages. This language setting controls the language of the product except for the login page.

Data formatting and report languages are available in the following cultures in the **Change Locale** list:

Table 147. Languages in the Change Locale list and the cultures that they represent	
Language in the Locale list	Culture
French	French (France)
German	German (Germany)
Italian	Italian (Italy)
Japanese	Japanese (Japan)
Portuguese	Portuguese (Brazil)
Spanish	Spanish (Spain)
Simplified Chinese	Chinese (China)
Traditional Chinese	Chinese (Taiwan)
U.K. English	English (UK)
U.S. English	English (US)

Considerations for specific languages

When OpenPages with Watson is set to use U.S. English, dates are formatted as mm/dd/yy. For example, January 3, 2020, is formatted as 1/3/20 rather than 03/01/2020 in U.K. English.

When the product is set to use Spanish (Spain), numbers are formatted as 123.456,78, where the period is a thousands separator and the comma is used as a decimal separator. For example, the number twelve thousand and five hundred is formatted as 12.500 in Spanish (Spain) rather than 12,500 in Spanish (Mexico).

In several cultures, the convention is to place the currency symbol after the number. In OpenPages with Watson, currency symbols are always displayed before the number.

Date formatting can be unconventional as well.

Localizing object text

Object text is the descriptive label name that displays in the application for object types, object fields, filters, and enumerated values. You can translate and modify object text for a specific locale.

For a list of supported locales, see the topic, [Chapter 18, “Localizing text,” on page 443](#).

You can modify the following object text for a locale:

- The singular and plural labels that display the name of an object type, such as "Risk" and "Risks" for the Risk object type, wherever that object type appears in the application. For more information, [“Modifying object text” on page 445](#).
- A singular label that displays:
 - The name of an object field in an object view.
For example, if you had an object field called "Impact" that displayed the label text "Impact", you could change the label text to display "Severity of impact" instead.
 - The values of an enumerated field.

Note:

- Only plain text should be entered as object text in labels. Light formatting is supported for field guidance text strings. HTML and line breaks are not supported.
- Object text has a 4000 character maximum per label.

Object text is grouped primarily by object type with an additional group for unassigned field groups.

For example, the SOXControl group contains the label text for the Control object and its related field groups.

The Unassigned Field Groups group contains the label text for field groups that are either not assigned to an object type or are commonly used by all object types, such as System Fields, Currency Attributes, Publishing, and so forth.

Important: Do not change or translate currency codes.

Modifying object text

You can modify object text strings for object types, object fields, filters, and enumerated values.

About this task

To do this task, you need the **SOX > Administration > Object Text** application permission.

The **Category** column on the **Object Text** page describes what type of text the object type contains.

Table 148. Using the Category column	
If the Category column is...	The object text defines ...
Enum Value	Label text for an enumerated value for an object field
Field	Label text and field guidance for an object field

Table 148. Using the Category column (continued)

If the Category column is...	The object text defines ...
Filter	Label text for a public filter
Object	Singular and plural forms of the displayed label text for an object type

Procedure

1. Click  > **System Configuration** > **Object Text**.
2. To find object text that you want to view or modify, click  to access the search filter.
 - a) Select one or more object types in **Object Type**.
 - b) Select one or more filters in **Search Scope**.
 - c) Optional: Click in the Search box and enter free text. The search returns results when it finds a match in the item, description, or labels in any language. You can enter single words. For example, enter "audit" to find all object texts with the word "audit" in the item, description, or labels. The Search box text is not case-sensitive.
3. To modify labels for an enumerated value for an object field:
 - a) Click the row for the enumerated value object text that you want to update (the **Category** column is **Enum Value**).
 - b) For selected locales, enter text in **Label**.

If it is displayed, click  to populate translated values to languages. For more information, see ["IBM Watson Language Translator" on page 847](#).
 - c) Click **Done**.
4. To modify labels and guidance for an object field:
 - a) Click the row for the object field text that you want to update (the **Category** column is **Field**).
 - b) For selected locales, enter text in **Label** and **Guidance**.

If it is displayed, click  to populate translated values to languages. For more information, see ["IBM Watson Language Translator" on page 847](#).
 - c) Optional: Apply formatting in **Guidance**. For more information, see ["Applying light formatting to text" on page 283](#).
 - d) Click **Done**.
5. To modify labels for a filter:
 - a) Click the row for the filter that you want to update (the **Category** column is **Filter**).
 - b) For selected locales, enter text in **Label**.

If it is displayed, click  to populate translated values to languages. For more information, see ["IBM Watson Language Translator" on page 847](#).
 - c) Click **Done**.
6. To modify labels for an object type:
 - a) Click the row for the object type that you want to update (the **Category** column is **Object**).
 - b) For selected locales, enter text in **Singular Label** and **Plural Label**.

If it is displayed, click  to populate translated values to languages. For more information, see ["IBM Watson Language Translator" on page 847](#).

IBM Watson Language Translator can correctly translate singular and plural text.

- c) Click **Done**.

Localizing system fields

You can change the system fields used for unassigned field groups that are specific to a locale. This change affects all object types and views.

For a list of supported locales, see [Chapter 18, “Localizing text,” on page 443](#).

Procedure

1. Click  > **System Configuration** > **Object Text**.
2. Click  to access the search filter.
3. Click **Unassigned Field Groups** in **Object Type**.
4. Click **System Fields** in **Search Scope**.
5. Select the name of the field that you want to change.
6. Click the name of the locale code you want to change, for example, en_US.
7. Make the required changes.
8. Click **Done**.

Localizing application text

Application text is the descriptive label names for core parts of the system.

Application text is static, which means that it is unlikely to change over time. You can modify application text that is specific to a locale. For list of supported locales, see [Chapter 18, “Localizing text,” on page 443](#).

Application text applies to core parts of the system while object text applies to text strings that are specific to object types, for example, object names, fields names, and so on. For more information about object text, see [“Localizing object text” on page 445](#).

You can modify locale-specific application text for:

- The text label that displays for an application text.
- The format for the display of names and numeric data. For examples, see [“Modifying the bucket heading format of the phonebook” on page 449](#) and [“Modifying how the names of users are displayed” on page 450](#).

Note: Application label text is limited to 4000 characters. Application text names and descriptions are limited to 256 and 2048 characters, respectively.

The following table shows the groupings by folder category for application text:

Table 149. Application text folder categories	
This folder	Contains the label text for
Application Messages	Messages that are displayed for dependent fields and pick lists, and System Admin Mode.
Buttons	The icons that are used within the application. For example, com.button.back contains the text for the Back icon, com.button.copy contains the text for the Copy icon.

Table 149. Application text folder categories (continued)

This folder	Contains the label text for
Column Headings	The table column headings that are used, albeit rarely, in the object views in the UI and in JSP Notification Manager reports For example, com.column.heading.start.date contains the text for the Start Date column, jspreports.notification.tests.column.parent contains the text for the Parent column in the JSP Notification report.
Custom	User-defined keys. For more information, see “Creating a custom setting” on page 499 .
Email Templates	Text strings that are part of email notifications.
Exceptions	Messages that are displayed to users when an error condition occurs. For example, com.exception.object.profile.not.found contains the text for the error message displayed when a profile is not found, exception.file.delete contains the text for the error message displayed when a user does not have permission to delete a file.
Formats	The formatting of numeric and name display text. For details, see “Modifying application text ” on page 449 .
Labels	Objects that are not considered objects, such as administrative tasks, and configuration objects. For example, app.manage.files.field.access.control.read contains the text for the Read property for system folders, app.workflow.email.label contains the text displayed on the email tab in the workflow action properties pane.
Menu Items	Links to other items that are not listed on the Primary menu or the Administration menu. For example, app.calculation.action.set.field.option contains the text for the Set Field item for calculations.
Miscellaneous	A variety of objects that do not belong to other groups. Includes label text for such objects as guided action, page footer, reporting status, notification messages, and so forth.
Reporting Framework	Objects that are used by the Reporting Framework.
Table Headings	(no longer used)
Titles	The initial portion of the breadcrumb trail.
Validation Messages	Messages that are displayed to users when invalid information has been entered in a field or to confirm a specific user action such as entering or exiting System Admin Mode or deleting any objects. For example, com.validation.logon.username.required contains the message text displayed when a user name is missing such as when it is created or when a user logs on, file.delete.confirmText contains the text in the confirmation prompt window that displays during a delete operation.

Modifying application text

You can modify the value of the displayed label or text for any application object (such as icons, labels, report names and descriptions, messages). The process for modifying display text is the same for all application objects, including reports.

About this task

To do this task, you need the **SOX > Administration > Application Text** application permission.

Changes to the displayed text appear wherever the particular object is displayed in the application.

Procedure

1. Click  **System Configuration** > **Application Text**.
2. To find application text that you want to view or modify, click  to access the search filter.
 - a) Select one or more categories in **Search Scope**.
 - b) Optional: Click in the Search box and enter free text. The search returns a results when it finds a match in the name, description, or values in any language. You can enter single words. For example, enter "path" to find all application texts with the word "path" in the name, description, or values. The Search box text is not case-sensitive.
 - c) Locate the application text that you want to modify.
3. To modify application text, click an application text in the list. Make your changes in one or more locales.

If it is displayed, click  to populate translated values to languages. For more information, see ["IBM Watson Language Translator" on page 847](#).

4. Click **Done**.
5. To add new application text, click **New**.
 - a) Enter a **Name**.
Allowed characters are A-Z, a-z, 0-9, period, underscore, hyphen, and spaces. Special characters are not allowed.
 - b) Select a **Category**.
 - c) Enter a **Description**.
 - d) Enter a **Default Label**.

If it is displayed, click  to populate translated values to languages. For more information, see ["IBM Watson Language Translator" on page 847](#).

- e) In the locale code that you want to modify, for example, French or Japanese, enter text for that language.

If you neither click  nor enter text for each locale code, the text in **Default Label** is populated to all languages.

- f) Click **Create**.

Modifying the bucket heading format of the phonebook

You can modify the format of the bucket heading in the phonebook style User selector for a locale. The selector is visible only on administrator pages for users and groups. It is not visible to end users.

Note: You can also modify the bucket size of the phonebook. For more information, see [“Actor selectors: Configure the bucket size of the phonebook” on page 482](#).

Procedure

1. Click  > **System Configuration** > **Application Text**.
2. Click  to access the search filter.
3. Click **Formats**.
4. Click the **com.user.bucket.name.format** application text.
5. Click the name of the locale code you want to modify, for example, **en_US**.
6. Modify the format. The default format is {0} - {1}.

The format string uses Java code. Generally, the {0} in the format string is a variable that is replaced by the name of the target object.

7. Click **Done**.

Example

To display a bucket heading with the name of the first person in the bucket followed by a dash and then the name of the last person in that bucket, you would enter the following codes in the Label field: {0} - {1}.

Modifying how the names of users are displayed

You can control how the names of users are displayed for a locale. The default is given name (first name) and surname (last name) in bold, then email in regular font.

When you change the display format, the change occurs throughout the application wherever the person's name displays. For example, if you modify the display format so that the last name of the person is followed by the person's first name, that modified name format displays in user selector fields when you search for users.

Note: If an invalid format string is defined, only the username is displayed.

Procedure

1. Click  > **System Configuration** > **Application Text**.
2. Click  to access the search filter.
3. Click **Formats**.
4. Click the **com.display.name.format** application text.
5. Go to the locale code you want to modify, for example, **en_US**.
6. Modify the format as follows:

To display this name format...	Type this code...	
Username	%NM;	Displays the value in the User Name field on the User Information page.
First Name	%FN;	Displays the value in the First Name field on the User Information page.
Last Name	%LN;	Displays the value in the Last Name field on the User Information page.

To display this name format...	Type this code...	
Email	%EM;	Displays the email address of a user in the Email object field on a User Information page.

Combinations and special characters are allowed, except for the hyphen (-) character.

- For a field that is in an editable state, a hyphen applies bold formatting to the text in front of the hyphen.
- For a field that is in a read-only state, a hyphen shortens the display name. Only the text before the hyphen is displayed. The full display name is displayed in a tooltip when a user clicks the user icon.
- The hyphen character is not displayed in the user interface.

The following table shows a field in an editable state, a read-only state, and in a read-only state with the tooltip displayed. This example uses the %FN; %LN; - %EM; display format:

Editable state	Read-only state	Tooltip
* Owner * Sam Adams sam.adams@fed.gov Search users	* Owner * Sam Adams	* Owner * Sam Adams sam.adams@fed.gov

7. Click **Done**.

Example

Assume that a user is defined where **User Name** is "jsmith", **First Name** is "Jane", and **Last Name** is "Smith".

If com.display.name.format is set to ...	The user displays as ...
%NM;	jsmith
%FN;	Jane
%LN;	Smith
%FN; %LN;	Jane Smith
%FN; %LN; - %EM;	Jane Smith jsmith@co.com
%FN; %LN; - %NM;	Jane Smith jsmith
%FN; %LN; (%NM;)	Jane Smith (jsmith)
%FN; %LN; [%NM;]	Jane Smith [smith]
%NM; - %FN; %LN;	jsmith Jane Smith

Defining messages and behavior on the login screens

You can define messages that are displayed on the login screen for OpenPages and configure certain behavior.

About this task

The login screen can contain the following messages:

- A system notice

Can be any text, for example, OpenPages will be unavailable on Sunday 8:00-14:00 due to system maintenance.

- Checkbox text

Can be any text, for example, I have read the privacy statement and I agree to the terms and conditions. The user must click the checkbox to log in.

- A privacy statement

Can be any text, for example, a company-wide statement about terms and conditions or privacy.

- A privacy statement link

Contains a link, for example, to an intranet site with more information about privacy. The link opens in a new tab.

The link is also used by the **Privacy** menu item in the Help menu.

- An acceptable use policy link

Contains a link, for example, to an intranet site with more information about acceptable use. The link opens in a new tab.

The link is also used by the **Acceptable Use** menu item in the Help menu.

You define a message's content by using application text strings. If a string is empty, the message is not displayed.

The following example shows all the messages. The numbers correspond to the application text strings listed in Table 150 on page 453.

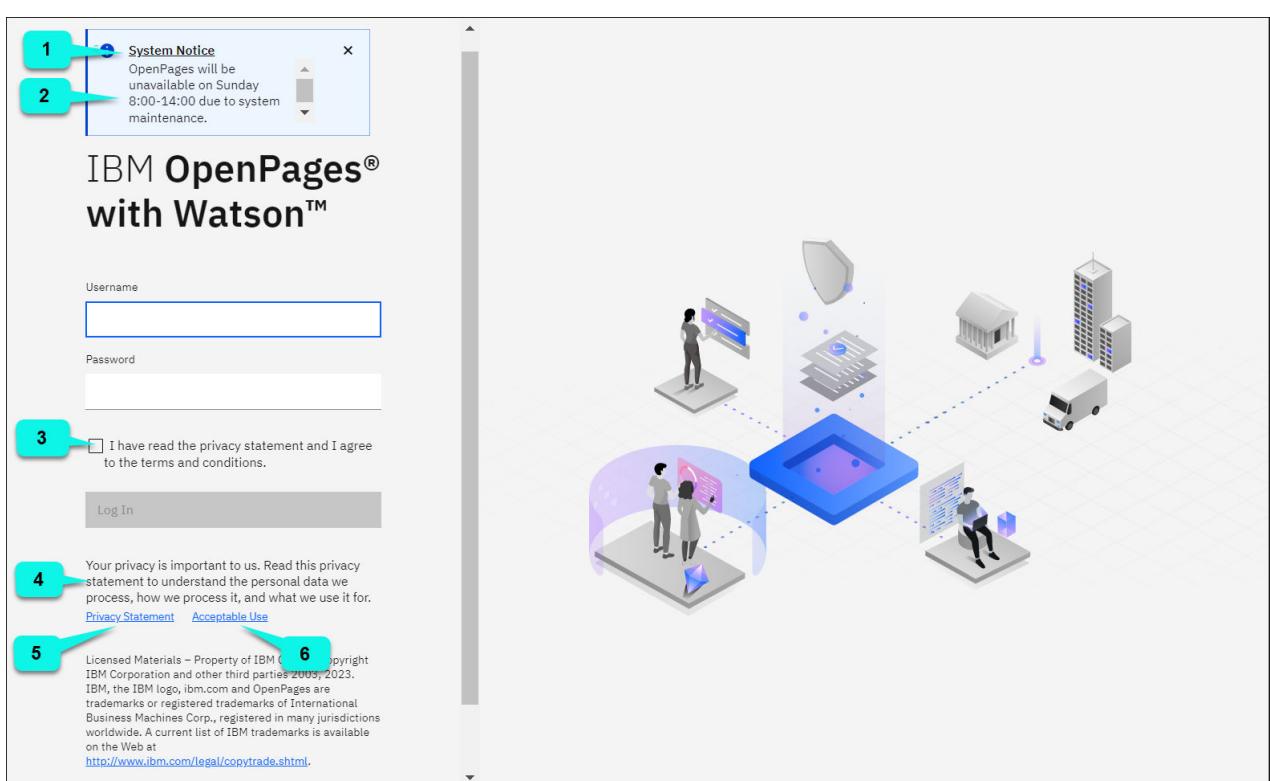


Figure 61. Login screen messages and application text strings

Table 150. Messages and application text strings

#	Description	Located in the Application Text > Labels category
1	Title for a system notice. The default is System Notice.	com.label.logon.system.notice.header
2	Text for a system notice. If empty, the system notice box, including the system notice header, is not displayed. Default is empty.	com.label.logon.system.notice.text
3	Text displayed next to the checkbox. If empty, the checkbox and corresponding text is not displayed. Default is empty.	com.label.logon.checkbox.text
4	Text for a privacy statement. Default is empty.	com.label.logon.privacy.text
5	Title for a privacy statement link. Default is Privacy Statement. The link is displayed if a URL is defined in the Privacy Link URL registry setting.	com.label.logon.privacy.link
6	Title for an acceptable use policy link. Default is Acceptable Use. The link is displayed if a URL is defined in the Acceptable Use Link URL registry setting.	com.label.logon.acceptable.use

The placement of the messages on the login screen is fixed and cannot be changed.

[Figure 61 on page 452](#) is the login screen.

Each locale can have one message. The user's locale determines the message that is displayed. The message that is defined in the en_US locale is the default message if the user's locale is not saved in the browser.

Note: The messages are displayed before users log in to OpenPages. Ensure that the content of the messages is appropriate for users who might not have access to OpenPages.

If you are using single sign-on (SSO), the login screen is bypassed. However, users still see the messages.

- If only a system notice is defined, the system notice is displayed on the dashboard when users access the system. The system notice is displayed once per session. Changes are not immediately broadcast. The system notice header that is defined in **com.label.logon.system.notice.header** is not displayed on the dashboard.
- Otherwise, the messages are displayed on a blank page in OpenPages with a **Continue** button. If you defined checkbox text, users must click the checkbox to enable the **Continue** button. When users click **Continue**, they can access OpenPages.

For example, if you define a system notice and checkmark text, users see a page that is similar to the following page:

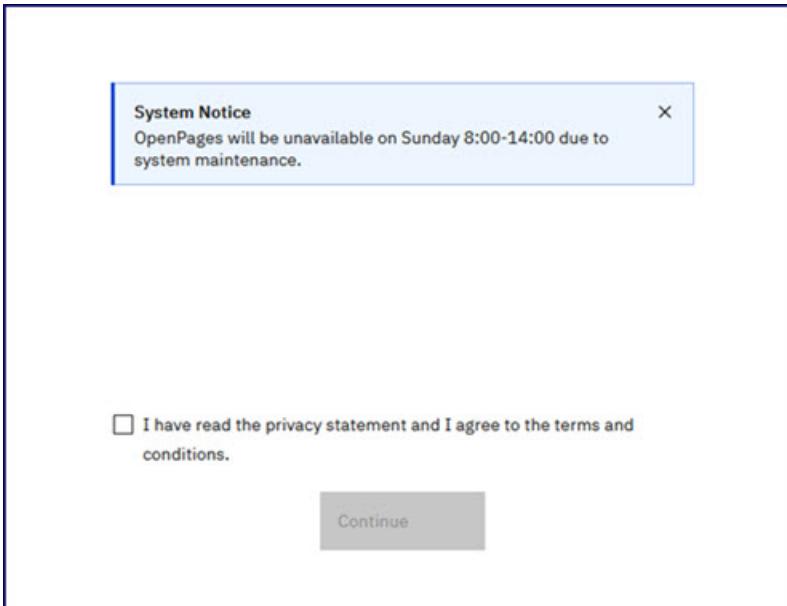


Figure 62. A system notice and checkmark text displayed for SSO users

You can optionally add HTML formatting when you define application text strings, for example:

- text displays text in bold.
- text displays text in italics.
-
 begins a new line.
- link_text inserts a link.

For example: My test link

Procedure

1. Click > **System Configuration** > **Application Text**.
2. Click to access the search filter.
3. Click **Labels**.
4. Search for one of the following labels. Click the link to edit the application text.
 - **com.label.logon.system.notice.header**
 - **com.label.logon.system.notice.text**
 - **com.label.logon.checkbox.text**
 - **com.label.logon.privacy.text**
 - **com.label.logon.privacy.link**
 - **com.label.logon.acceptable.use**
5. Click the name of the locale code you want to modify, for example, **en_US**.
6. Add or edit message text.
7. Click **Done**.
8. If you defined a privacy statement link, specify the URL to display when users click the link.
 - a) Click > **System Configuration** > **Settings**.
 - b) Edit the **Applications > Common > Privacy Link URL** setting. Specify the URL of the privacy statement.
9. If you defined an acceptable use policy link, specify the URL to display when users click the link.

- a) Click  > **System Configuration** > **Settings**.
- b) Edit the **Applications** > **Common** > **Acceptable Use URL** setting. Specify the URL of the acceptable use policy.

What to do next

Log on to OpenPages and verify that the messages display.

Tip: To remove a message, repeat the steps and clear the text in the **Label** box. If you added a privacy statement link or an acceptable use policy link, clear the value of its registry setting.

The Custom folder

The **Custom** folder is a container for user-defined keys (such as values returned by computed fields, email text for Notification Reports, and values used by Survey reports).

The keys also provide a means for displaying localized text for reports (such as reports that are manually published).

Typically, this folder is populated through the ObjectManager tool. You can add new keys to the **Custom** folder from the **Application Text** page.

To modify localized display text for a key in the **Custom** folder, see “[Modifying application text](#)” on page [449](#).

Adding new keys

You can add new keys to the Custom folder for localization.

Note: For Cognos report pages (or JSP report instances) that were manually created using the publishing facility on the IBM OpenPages with Watson server, you can use the values in the Report Name Key and Report Description Key fields on the report page to manually create custom application text keys to localize the name and description of a report after it is created.

Procedure

1. Click  > **System Configuration** > **Application Text**.
2. Click  to access the search filter.
3. Click **Custom**.
4. Click **New**.
5. In the **Name** box, type the name of the key.
For example, a report called My Loss Events could have `report.name.my.loss.events` for a report name key or `report.description.my.loss.events` for a report description key.
6. Optionally, type a description of the key.
7. In the **Default Label** box, type the text that will be displayed, by default, if no translated text is provided.
8. Type the translated text you want displayed for each locale.
9. Click **Create**.

Chapter 19. Reporting periods, object resets, and rulesets

A reporting period is a "snapshot" of the current state of the repository, usually created when the documentation phase of a quarter or year is complete and ready for attestation. Object resets are a way to automatically modify objects that exist in the IBM OpenPages with Watson repository. Object resets are rule-based operations that are contained in a ruleset.

Reporting periods

Past reporting periods can be viewed and reported on at any time. Changes to the repository do not affect data in past reporting periods.

Users can view data, for example, in dashboards and for objects, for the current data (current state of the repository) and past reporting periods.

Object resets

The most common use of the object reset functionality is to "reset" all of your objects at the beginning of a new reporting period. For example, each quarter you have controls and tests that need to be reviewed and performed. The results of those tasks are recorded by updating the properties and attachments of the appropriate objects. After all quarterly tasks are completed, and the quarter is finished, you archive all of the results into a reporting period and prepare for the new quarter. However, the existing objects still display the test results and changed properties of the previous quarter. If you are planning to reset your data as part of the beginning of a new reporting period, you will have to archive the existing data to a reporting period.

Rather than modify the objects by hand, you can use the object reset capability to take your existing objects and modify their properties based on the rules in your ruleset.

While object resets work well with the reporting period capability of OpenPages with Watson, object resets do not require the existence of a reporting period to be used.

Reporting period interactions

You can interact with the reporting schema, the ACL, and the change history for a reporting period.

The reporting schema

By default, the reporting schema is only populated with the data from the current reporting period.

To populate the reporting schema with data from previous reporting periods you must enable the **Populate Past Periods** setting and re-create the reporting schema (see, ["Populating past reporting periods" on page 119](#)).

ACLs

When viewing objects, your existing ACLs control which objects you can view in the current reporting period and in past reporting periods. If your access permissions change in the current reporting period, you will be able to view the newly accessible items in past reporting periods, and you will not be able to view items to which you have lost permissions, even if in past reporting periods you had access to them.

Regardless of your access permissions, you are never allowed to add, edit or remove objects and/or files from past reporting periods.

The Activity tab

You can view the **Activity** tab for an object to see its change history. Only the changes made during the currently selected reporting period are shown. You can view the change history for past reporting periods, but only the change activities for that reporting period are shown.

You cannot view change histories for multiple reporting periods on the same **Activity** tab.

Using System Admin Mode with reporting periods

When you create, finalize, or delete reporting periods, you need to be in System Admin Mode (SAM).

For more information, see [“Enabling and disabling System Admin Mode” on page 37](#).

Reporting period permissions and settings

To manage reporting periods, the user performing the reporting period operation must belong to a group with the specific application permissions. The amount of time after a reporting period is created in which the reporting period can be deleted is set in the *Delete Interval* setting

Reporting period permissions

Administrators with the **Reporting Periods** application permission can create, modify, enable or disable, and delete reporting periods.

Deletion period setting

It is possible to configure the amount of time after a reporting period is created in which the reporting period can be deleted. This property is set in the *Delete Interval* setting and defaults to 7 days after the reporting period is created.

For details see, [“Modify the deletion interval for a reporting period” on page 479](#).

Creating a finalized a reporting period

You can create finalized reporting periods. When you finalize the current reporting period, a snapshot of the current reporting period is created. You then have the current reporting period and a finalized (or past) reporting period. You can have multiple finalized reporting periods.

Before you begin

To create a finalized reporting period, you must have the **Reporting Periods** application permission.

About this task

Create a finalized reporting period if no further data changes are expected.

Procedure

1. Click  > **Enable System Admin Mode**.
2. Click  > **System Configuration** > **Reporting Periods**.
3. Click **New Finalized**.
4. Enter the information and click **Create**.

The reporting period displays with a status of **Finalized**. You are not able to modify it without deleting the entire reporting period.

5. Click  > **Disable System Admin Mode**.

What to do next

You can use task views to view the data in the finalized reporting period. You can also use  > **Change Reporting Period** to select the reporting period.

Note: You might need to refresh the screen to see the **Change Reporting Period** menu item.

Disabling finalized reporting periods

Over time, you might have many finalized reporting periods. Some of them might not be needed for day-to-day operations, but you still want to keep them. In this case, you can disable the finalized reporting periods.

Before you begin

To do this task you must have the **Reporting Periods** and **System Administration Mode** application permissions.

About this task

You might want to disable older reporting periods to reduce the number of reporting periods that users see in the application. When a finalized reporting period is disabled, it is not available to users through the UI, such as through  > **Change Reporting Period**.

In addition, you might want to disable older reporting periods for performance reasons. Finalized reporting periods take up space in the database, which can slow down actions such as reporting schema generation.

The current reporting period cannot be disabled.

Procedure

1. Click  > **Enable System Admin Mode**.
2. Click  > **System Configuration** > **Reporting Periods**.
3. Locate the reporting period that you want to disable.
4. Click  , and then click **Disable**.

If  is not displayed, a background process might be running. To see a list of processes, click  > **Other** > **Background Processes**.

The past reporting period is now disabled.

Tip: You can enable a disabled reporting period. Click  > **Enable** to enable it.

5. Click  > **Disable System Admin Mode**.

Deleting a reporting period

After you create a finalized reporting period, occasionally you might need to delete it so that users can make last-minute changes to your financial close, or due to a mistake in the name (for example, wrong quarter, wrong year, and so forth).

You might also want to delete disabled reporting periods that are no longer needed.

The current reporting period can never be deleted.

A finalized reporting period can be deleted for a configurable amount of time after the reporting period is created. For details on this setting, see “[Modify the deletion interval for a reporting period](#)” on page 479.

- If the deletion period has **expired**, then the finalized reporting period cannot be deleted.
- If the deletion period has **not expired**, then the finalized reporting period can be deleted.

Note: The default period for deletion of a finalized reporting period is seven days after finalization.

Procedure

1. Click  > **Enable System Admin Mode**.
2. Click  > **System Configuration** > **Reporting Periods**.
3. Locate the reporting period that you want to delete.
4. Click , and then click **Delete**.
If **Delete** is not displayed, the deletion period for that reporting period has expired. However, you can retroactively change the deletion period setting.
If  is not displayed, a background process might be running. To see a list of processes, click  > **Other** > **Background Processes**.
5. Click  > **Disable System Admin Mode**.

Object resets

Object resets are a way to automatically modify objects that exist in the IBM OpenPages with Watson repository.

The most common use of the object reset functionality is to "reset" all of your objects at the beginning of a new reporting period. For example, each quarter you have controls and tests that need to be reviewed and performed. The results of those tasks are recorded by updating the properties and attachments of the appropriate objects. After all of these quarterly tasks have been completed, and the quarter is finished, you archive all of the results into a Reporting Period and prepare for the new quarter. However, the existing objects still display the test results and changed properties of the previous quarter.

Rather than go in and modify the objects by hand, you can use the object reset functionality to take your existing objects and modify their properties based on the rules in your ruleset.

While object resets work well with the reporting period capability of the OpenPages with Watson application, object resets do not require the existence of a reporting period to be used.

Object resets on file attachments

You can only use object resets to delete objects that are JSP-based, not attachments available when using the **Browse Files** option. For example, if you use an object reset on SOXDocument, you see the following error:

```
VALIDATION ERROR (Line: 8 Column: 55): Content Type (SOXDocument)
must be JSP-based to be referenced in an Object Delete rule.
```

Suppose that you have files that are attached to test results. You can configure the settings to delete attachments when test results are deleted. To delete the SOXDocument objects, you can add SOXDocument to the **Cascade Delete** setting to delete the files that are associated with the test results during the object reset rule to delete test results.

Object resets on system fields

When modifying fields or using fields within <criteria> tags, you may not use "system" fields. System fields are the fields common to all object types, such as name, description, or creator. Field modifications and ruleset criteria must use custom fields (non-system fields). If the field you want does not appear in a field group for the appropriate object type, you cannot use it in your ruleset.

Object resets on currency fields

If you use an object reset rule to update the value of the Local Currency Code of a currency field, the Exchange Rate and Base Amount are not updated to match the new Local Currency Code value.

While the Base Amount is calculated using the Local Currency Code and the Exchange Rate, it will not change because the Exchange Rate has not been modified and the number of displayed fraction digits for the currency has not been changed. In order to see a change in the Base Amount, you must include a rule to update the Exchange Rate or modify the number of displayed fraction digits.

Preparing your data

Before an object reset is performed, you will need to perform a few tasks to help ensure that the reset procedure goes smoothly.

- Back up your OpenPages with Watson data before running an object reset.
- If you plan on archiving your changes to a reporting period, you will need to set up the reporting period before running the object reset.

Creating a ruleset

Object resets are rule-based operations on the objects in your IBM OpenPages with Watson repository. The rules that govern how an object reset will affect your data are contained in a ruleset file.

A ruleset is a set of rules contained in an XML loader file that is created outside of the OpenPages with Watson application. Multiple rulesets can be included in a single XML file. The ruleset loader file is loaded into the system through the ObjectManager loader tool. After the ruleset is imported, it can be selected during the Specify Options step of the Object Reset guided action.

When you use ObjectManager loader tool to import security rules, the entire ruleset is loaded and replace existing security rules that have the same name as a imported rule. Before importing security rules, export your existing rules first.

Object Resets can modify objects in three ways: modifying the value of a property, deleting an object, and disassociating two objects.

When creating a ruleset, you must know the bundles, properties, and property values you are modifying and match them exactly. If you do not specify a valid property or property value, the property will not be modified.

Note: Before creating a final ruleset to use for your reset session, it can be extremely helpful to create simple rulesets that contain a single rule from your final ruleset. Running these single rulesets against a known data set can verify the accuracy of each rule before attempting a massive modification of your data.

To create the ruleset file, create a new XML file. Save the file with the following naming convention:

```
<file-identifier>-op-config.xml
```

Sample ruleset

The following XML is a sample ruleset.

```
<?xml version="1.0" encoding="UTF-8"?>
<openpagesConfiguration xmlFormatVersion="1.20">
    <ruleSets>
        <ruleSet name="Quarterly Reset"
            description="Rule set to be executed at the beginning of each
            and every quarter"
            type="Object Reset">
            <rule name="Rule 1">
```

```

        description="Property Update rule setting a property"
        type="Property Update">
      <propertyUpdateRule contentType="SOXControl">
        <bundle name="SOXControl">
          <property name="Design Effectiveness"
            useDefaultValue="false">
            <propertyValue name="Not Rated"/>
          </property>
        </bundle>
      </propertyUpdateRule>
    </rule>

    <rule name="Rule 2"
      description="Property Update rule setting a collection of
      properties (including a multi-valued one)."
      type="Property Update">
      <propertyUpdateRule contentType="SOXRisk">
        <bundle name="SOXRisk">
          <property name="Assertions"
            useDefaultValue="false">
            <propertyValue name="Existence"/>
            <propertyValue name="Rights and Obligations"/>
        </property>
        <property name="Impact"
          useDefaultValue="false">
          <propertyValue name="Unknown"/>
        </property>
      </bundle>
    </propertyUpdateRule>
  </rule>

  <rule name="Rule 3"
    description="Object Delete rule"
    type="Object Delete">
    <objectDeleteRule contentType="SOXTestResult"/>
  </rule>

  <rule name="Rule 4"
    description="Object Delete rule with criteria"
    type="Object Delete">
    <objectDeleteRule contentType="SOXIIssue"/>
    <criteria logicalOperator="or">
      <criterion bundle="SOXIIssue"
        property="Status"
        operator="=">
        <propertyValue name="Closed"/>
      </criterion>
    </criteria>
  </rule>

  <rule name="Rule 5"
    description="Object Disassociate rule"
    type="Object Disassociate">
    <objectDisassociateRule parentContentType="SOXRisk"
      childContentType="SOXDocument"/>
  </rule>

</ruleSet>
<!--sample Reset Ruleset for a currency property-->
<ruleSet name="Your_Ruleset_Name"
  description="Reset a currency property"
  type="Object Reset">
  <rule name="Reset a currency property"
    description=""
    type="Property Update">
    <propertyUpdateRule contentType="SOXAccount">
      <bundle name="OPSS-Account_Annualized Value">
        <property name="Annualized Value_LA"
          useDefaultValue="false">
          <propertyValue name="1.0"/>
        </property>
      </bundle>
      <bundle name="OPSS-Account_Annualized Value">
        <property name="Annualized Value_LC"
          useDefaultValue="false">
          <propertyValue name="AED"/>
        </property>
      </bundle>
      <bundle name="OPSS-Account_Annualized Value">
        <property name="Annualized Value_ER"
          useDefaultValue="false">

```

```
<propertyValue name="1.0"/>
</property>
</bundle>
</propertyUpdateRule>
</rule>
</ruleSet>
</ruleSets>
</openpagesConfiguration>
```

Ruleset tag library

Use the following XML tags to build a ruleset.

[openpagesConfiguration](#)

[ruleSets](#)

[ruleSet](#)

[rule](#)

[propertyUpdateRule](#)

[bundle](#)

[property](#)

[objectDeleteRule](#)

[objectDisassociateRule](#)

[criteria](#)

[criterion](#)

[propertyValue](#)

<openpagesConfiguration>

Description: Progenitor tag for the loader file contents. All other tags are contained within the <openpagesConfiguration> tag.

Parent Tags: None.

Child Tags: <ruleSets>

Syntax:

```
<openpagesConfiguration xmlFormatVersion="1.15">
</openpagesConfiguration>
```

Attributes:

- [xmlFormatVersion](#)

Version of the IBM OpenPages with Watson XML DTD.

<ruleSets>

Description: Container tag for one or more ruleSet tags.

Parent Tags: <openpagesConfiguration>

Child Tags: <ruleSet>.

Syntax:

```
<ruleSets>
</ruleSets>
```

Attributes: None.

<ruleSet>

Description: A ruleset is a collection of rules that will be executed when the ruleset is selected during a Reset session. Each ruleset is displayed in the IBM OpenPages with Watson user interface as a separate entry in the list of Rulesets.

Parent Tags: <ruleSets>

Child Tags: <rule>

Syntax:

```
<ruleSet name="Name"
         description="Description"
         type="Object Reset">
</ruleSet>
```

Attributes:

- name

An identifying name for the ruleset. Will be displayed in the OpenPages with Watson user interface. The maximum length for the ruleset name attribute is 255 bytes (not characters).

- description

A description of the function of the ruleset. The maximum length for the ruleset name attribute is 2000 bytes (not characters).

- type

The type of ruleset. Currently, there is only one type - "Object Reset".

<rule>

Description: Each <rule> tag contains a single rule that will be applied to the IBM OpenPages with Watson data when the ruleset is selected and a Reset session is initiated.

Parent Tags: <ruleSet>

Child Tags: <propertyUpdateRule>, <objectDeleteRule>, <objectDisassociateRule>, <criteria>

Syntax:

```
<rule name="Name"
      description="Description"
      type="[Property Update|Object Delete|Object Disassociate]"
</rule>
```

Attributes:

- name

The name of the rule. The maximum length for the rule name attribute is 255 bytes (not characters).

- description

A description of the function of the rule. The maximum length for the rule name attribute is 2000 bytes (not characters).

- type

The type of rule. There are three types of rules: Property Update, Object Delete, and Object Disassociate.

<propertyUpdateRule>

Description: The <propertyUpdateRule> tag defines a rule that modifies the value of an existing property on a certain object type. Unless modified by the use of the <criteria> tag within the same <rule> tag, all objects of the specified object type within the scope of the Reset will be updated.

Parent Tags: <rule>

Child Tags: <bundle>

Syntax:

```
<propertyUpdateRule contentType="">
</propertyUpdateRule>
```

Attributes:

- contentType

Specifies the object type that the rule will be applied to. Must match a valid IBM OpenPages with Watson object type.

<bundle>

Description: The <bundle> tag specifies which bundle contains the property to be modified.

Parent Tags: <propertyUpdateRule>

Child Tags: <property>

Syntax:

```
<bundle name="">
</bundle>
```

Attributes:

- name

The name of the bundle whose property will be modified.

<property>

Description: The <property> tag is used inside a <bundle> tag to specify the property that will be updated.

Parent Tags: <bundle>

Child Tags: <propertyValue>

Syntax:

```
<property name="">
  useDefaultValue="[true|false]"
  [<propertyValue>
    <propertyValue>]
</property>
```

Attributes:

- name

The name of the property to be updated.

- useDefaultValue

Specifies whether the property should be updated to reflect the default value of the property (if one exists). If no default value exists, the property is not updated.

<objectDeleteRule>

Description: The <objectDeleteRule> tag is used to specify an object type for deletion. Unless modified by the use of the <criteria> tag within the same <rule> tag, all objects of the specified object type within the scope of the Reset will be deleted.

Parent Tags: <rule>

Child Tags: None.

Syntax:

```
<objectDeleteRule contentType="" />
```

Attributes:

- contentType

Specifies the object type to be deleted. All objects of this type within the scope of the Reset are deleted.

<objectDisassociateRule>

Description: The <objectDisassociateRule> tag is used to disassociate an object type from another object type. If you use the <criteria> tag with this rule type, the criteria must be based on the child's property values. You cannot base a rule on properties or property values belonging to the parent object type.

Parent Tags: <rule>

Child Tags: None.

Syntax:

```
<objectDisassociateRule parentContentType="" childContentType="" />
```

Attributes:

- parentContentType

Identifies the parent object type that the child object type is associated with.

- childContentType

Identifies the child object type to be disassociated. Any objects of the child object type associated with objects of the parent object type within the scope of the Reset will be disassociated from the parent object.

<criteria>

Description: The <criteria> tag is used to refine the behavior of a rule by specifying the standards that need to be met in order to invoke the rule. The criteria tag can contain one or more <criterion> tags that will be judged when deciding whether to apply the rule to a specific object.

It should be noted that criteria can only be applied in a "positive" manner - that is, if the criteria are met, the rule will be used. You cannot specify a rule where if the criteria are met, the rule is NOT applied.

Parent Tags: <rule>

Child Tags: <criterion>

Syntax:

```
<criteria logicalOperator="[and|or]">
```

Attributes:

- logicalOperator

Specifies whether all of the criterion ("and") will be used to determine whether the rule will be applied to the object, or if only one of the criterion ("or") needs to be satisfied.

<criterion>

Description: The <criterion> tag allows the user to specify a property and value(s) that must match the evaluation specifications set in the <criterion> tag.

Use a maximum of three criterion within a single <criteria> tag. Adding additional criterion will increase the processing time required to complete the Reset.

Parent Tags: <criteria>

Child Tags: <propertyValue>

Syntax:

```
<criterion bundle=""  
          property=""  
          operator="[=|<|>|=|<=|<|>|=|like]"  
          <propertyValue="" />  
          [<propertyValue="" />]  
</criterion>
```

Attributes:

- bundle

The property bundle containing the property to be evaluated.

- property

The property name of the property to be evaluated.

- operator

Specifies the manner in which the value of the property will be evaluated. Valid operators are equal (=), not equal (<>), greater than (>), less than (<), greater or equal to (>=), less than or equal to (<=), and "like".

Only the equal, not equal, and "like" operators can be used with string variables.

Note: The "like" parameter allows the use of wild cards in the <propertyValue> tag. These wild cards consist of the "%" and "_" symbols, which are passed to a SQL database query against the database. The percent mark (%) symbol is used to represent any number of characters in a location, while the underscore (_) character is used to represent any single character in a location.

For SQL tool information, see the *Database tool information* topic at [“Introduction” on page xxi](#).

Note: The <propertyValue> referenced in a <criterion> tag cannot be null (or empty).

<propertyValue>

Description: The <propertyValue> tag performs two functions, depending on its location. The Boolean property value must be all lowercase. For example, "true" is correct, "True" is incorrect.

If the <propertyValue> tag is contained inside a:

- <property> tag, it specifies the new value (or values) for the updated property.
- <criterion> tag, it specifies the relevant property to be considered when applying the criteria.

Note: The <propertyValue> referenced in a <criterion> tag cannot be null (or empty).

If you are modifying an enumerated string (drop-down list) property that is multi-selectable, you can place multiple <propertyValue> tags inside the <property> tag. When the rule is processed, all of the <propertyValue> tags will be evaluated, and the property will be modified to select all of them.

Parent Tags: <property>, <criterion>

Child Tags: None.

Syntax:

```
<propertyValue name="" />
```

Attributes:

- name

Specifies the value of the property. The maximum length for the property value's name attribute is 2000 bytes (not characters).

Loading the ruleset

After you have finished creating the ruleset loader file, you will need to use the ObjectManager tool to load the ruleset into the IBM OpenPages with Watson system.

If you load a ruleset with the same name as an already-loaded ruleset, the ruleset will be overwritten with the new rules. To return to an earlier version of the ruleset, you would have to re-load the original ruleset loader file. Rulesets are not "version-controlled".

Procedure

1. Open a command or shell window on the OpenPages with Watson server.
2. Navigate to the <OP_Home> directory.

Where: <OP_Home> represents the installation location of the OpenPages with Watson application. By default, <OP_HOME> is c:\IBM\OpenPages on Windows or /opt/IBM/OpenPages on Linux.

3. Run the following command on a single line:

```
ObjectManager load config OpenPagesAdministrator <password> <path-to-ruleset-XML-file>
<file-identifier>
```

where

<password> is the password to the OPAdministrator user account.

<path-to-ruleset-XML-file> is the full path to the ruleset file you created.

<file-identifier> is the portion of the ruleset file name preceding "-op-config.xml". For example, if you created a ruleset file called "ruleset-op-config.xml", the <file-identifier> in the ObjectManager command is "ruleset".

4. The ruleset is now loaded. If you created multiple ruleset files, repeat this procedure for each of them.
5. If you encounter errors, read the log file to determine the cause of the error and fix it, then re-run the command in Step 2.

Performing the object reset

After you load the ruleset that you are using for the Object Reset, you must log in to the system and begin the Reset.

Access permissions and access

The user who runs the Reset must have the Object Reset application permission and the proper access to modify the data.

If the user does not have the Object Reset permission, they are not able to see Object Resets on the menu.

Configuring the ruleset parameters

Before running the Reset, there are some configuration parameters that should be set. In general, these settings need to be set only one time before your first time initiating a Reset, but you may want to change them for different entity trees or ruleset behavior.

Access the following Object Reset settings in the **Applications > Common > Object Reset** folder:

- **Logging Level** - this setting controls how much information is displayed. For configuration details, see “[Changing the logging level](#)” on page 494.
- **Check ACL** - this setting controls whether the Reset occurs against all or only some of the objects contained within the scope of the Reset session. For configuration details, see “[Obeying ACL restrictions](#)” on page 494.
- **Ignore Locks** - this setting controls whether existing locks on objects are honored when running the Reset. For configuration details, see “[Obeying locking restrictions](#)” on page 494.
- **Continue on Error** - this setting controls whether the Reset session will log errors and continue to run or halt processing. For configuration details, see “[Continuing on error](#)” on page 494.

Starting the object reset

When you reset objects, watch the status of the job and review the results for errors and warnings.

About this task

When you reset objects, watch the status of the session and review the results for errors and warnings.

The possible values for the **Status** field are Initiated, In Progress, Completed, or Failed.

The “Failed” status is shown only if the system is set to stop the reset if errors are encountered. If the system is set to continue on errors, then when the reset is completed, the “Completed” status is shown. Any errors that occurred during the reset are captured in the Reset Session Log.

Note: If you have chosen to obey ACL restrictions, the user must have the permissions to modify the objects within the scope of the Reset. If the user does not have sufficient permissions, warning messages will be generated in the log, and the objects will not be modified.

Procedure

1. Click  > **System Configuration > Object Resets**.
2. Click **New Reset**.
3. Enter a name and description for the new reset.
4. Select a ruleset from the list of available rulesets.
5. Click Choose next to **Reset Scope**.
6. Choose the Business Entities to which the Reset will be applied by selecting the check boxes next to the entity names. Click **Done**.
7. Click **Start Reset**.
The reset starts.
8. Track the progress of the reset session by monitoring the **Status** column of the table.

Results

When the reset session is finished, a new reset session is added to the list.

What to do next

Click the reset session and review the results:

- Click the **Information** tab to view object reset details. For information, see “[Viewing reset session detail information](#)” on page 470.
- Click the **Log** tab to view errors and warnings. For information, see “[Viewing reset session log information](#)” on page 470.

Refresh the reporting database. For information, see “[Refreshing the reporting database after the reset](#)” on page 471.

Viewing reset session detail information

You can view details about a reset session that is finished.

Click the name of an object reset session. The following information is displayed:

Name - The name of the Reset Session.

Description - The description of the Reset Session (set during the creation procedure)

Ruleset Name - The name of the Ruleset that was applied during this session.

Created - The time and date the Reset Session was created.

Start Date - The time and date the Reset began.

End Date - The time and date the Reset finished.

Status - The current status of the Reset. The Status can be one of the following values:

- Initiated - The Reset has been initialized, and is preparing to modify your data.
- In Progress - The Reset is currently modifying the selected data.
- Completed - The Reset finished successfully. Depending on whether the Reset was set to continue on errors, some errors may be reported in the Session Log.
- Failed - The Reset did not finish, because errors were encountered. Check the Session Log for details on what errors occurred.

Created By - The user that initiated the Reset Session.

Scope - The Business Entities that were modified by the Reset.

Logging Level - The level of detail that will be displayed in the Session Log. Can be one of the following values:

- Low - display error messages only
- Medium - display any error messages and any warning messages.
- High - display any errors, warnings, and any informational or diagnostic messages.

Continue on Error - Whether the Reset Session will log errors and continue to run, or whether the error will be logged and the session will halt. Value will either be “true” or “false”.

Check ACLs - Whether the Reset occurs against all objects contained within the scope of the Reset session, or whether the Reset occurs against only those objects that the user who initiated the Reset has access to. It can have a value of “true” or “false”.

Ignore Locks - Whether existing locks on objects are honored when running the Reset. A value of “true” means that locks were ignored when running the Reset, and a value of “false” means that locked objects were not modified by the Reset.

Viewing reset session log information

You can view log information about a reset session that is finished.

The level of detail depends on the configuration setting. For details on setting the logging level, see the topic “[Performing the object reset](#)” on page 468.

Procedure

1. Click  > **System Configuration** > **Object Resets**.
2. Click the object reset session.
3. Click the **Log** tab.

The reset session log contains three sections - the error messages section, the warning messages section, and the informational messages section.

Refreshing the reporting database after the reset

After you perform an object reset, refresh the reporting database so that users who run third-party reports will immediately see the changes.

If your users are using the reporting schema, you do not need to perform a reporting schema refresh. The IBM OpenPages with Watson reports will automatically see the changes.

For detailed information on performing a reporting database refresh, see [Chapter 7, “Managing the reporting schema ,” on page 117](#).

Exporting rulesets to an XML file

You can export all of the object reset rulesets to an XML file using ObjectManager. In order to do this, you must have file access to the IBM OpenPages with Watson server.

This procedure will export ALL defined rulesets. Exporting rulesets does not remove them from the OpenPages with Watson application; they will still be available for use after they are exported.

Procedure

1. Back up the `ObjectManager.properties` file.

Note: The `ObjectManager.properties` file is located in the root installation folder of your OpenPages with Watson installation. By default, this is `c:\OpenPages`.

2. Open the `ObjectManager.properties` file in a text editor.
3. Locate the following block of settings in the file:

```
configuration.manager.dump.modules=true
configuration.manager.dump.file=true
configuration.manager.dump.bundle.types=true
configuration.manager.dump.file.upload.content.types=true
configuration.manager.dump.jsp.based.content.types=true
configuration.manager.dump.content.type.relationship.sets=true
configuration.manager.dump.app.permissions=true
configuration.manager.dump.actors=true
configuration.manager.dump.actor.group.memberships=true
configuration.manager.dump.actor.object.profile.associations=true
configuration.manager.dump.non.form.based.resources=true
configuration.manager.dump.form.based.content.types=true
configuration.manager.dump.form.based.resources=true
configuration.manager.dump.channels=true
configuration.manager.dump.resource.sets=true
configuration.manager.dump.associated.resources=false
configuration.manager.dump.rule.sets=true
configuration.manager.dump.rule.set.execute.sessions=true
configuration.manager.dump.registry=true
configuration.manager.dump.object.profiles=true
configuration.manager.dump.locales=true
configuration.manager.dump.application.string.key.categories=true
configuration.manager.dump.application.string.keys=true
configuration.manager.dump.application.strings=true
configuration.manager.dump.error.strings=true
configuration.manager.dump.object.strings=true
configuration.manager.dump.job.types=true
configuration.manager.dump.currency.exchange.rates=true
```

```
configuration.manager.dump.currencies=true  
configuration.manager.dump.querydefinitions=true
```

4. Modify each line to have a `false` value, except the line that reads:

```
configuration.manager.dump.rulesets=true
```

5. Make sure that the following setting has a value of `false`:

```
configuration.manager.migrate.configuration.objects
```

6. Save the file and exit the editor.
7. Open a Command Prompt window.
8. Navigate to the `<OP_Home>` directory.

Where:

`<OP_Home>` is the installation location of the OpenPages with Watson application. By default, this is `c:\OpenPages`.

9. Run the following command on a single line:

```
ObjectManager dump config OpenPagesAdministrator <password>  
<path-to-xml-file> <file-identifier>
```

where

<password> is the password to the OPAdministrator user account.

<path-to-XML-file> is the full path to the ruleset file you created.

<file-identifier> is the portion of the ruleset file name preceding `-op-config.xml`. When the XML file is created, the file name will append `-op-config.xml` to the end of the filename. For example, if you specified a **<file-identifier>** called "ruleset", the generated XML file would be named "ruleset-op-config.xml".

10. A new XML file is generated in the specified location that contains only the latest version of the rulesets that exist in the application at the time of the export.

Note: Be sure to "reset" the `ObjectManager.properties` file to its original contents - otherwise, your scheduled backups using ObjectManager will only export the rulesets.

Chapter 20. Viewing the Configuration and Settings page

Settings control the functionality of numerous aspects and features in IBM OpenPages with Watson.

For information about working with settings in data loader files, see [“Paths for settings in data loader files” on page 474](#).

Managing settings

Use **Settings** to modify the values for predefined settings and add, copy, and delete custom settings.

Before you begin

To access **Settings**, you must have the Settings application permission set on your account.

About this task

You can modify the values for predefined settings. Do not delete any of the OpenPages predefined settings. These settings are required and cause unexpected behavior in the application if they are removed.

You can add your own custom folders and settings. The **New Setting** and **Delete** icons are hidden by default. Set both **/Applications/Common/Configuration>Show Hidden Settings** and **/Applications/Common/Configuration/Allow Create and Delete Settings** to **true** to add and delete settings. You can copy individual settings to another location and copy folders to new folders. When you copy a folder, you can give the new folder a name. The settings and subfolders in the folder are copied to the new folder.

Procedure

1. Click  > **System Configuration** > **Settings**.
2. To find a setting that you want to view or modify, click  to access the search filter.
 - a) Select one or more folders in **Search Scope**.
The folder path is displayed.
 - b) Optional: Click in the Search box and enter what you want to search for. The search returns results when it finds a match in the name, description, or value of a setting. You can enter single words. For example, enter **hidden** to find all settings with the word "hidden" in the name, description, or value.
The Search box text is not case sensitive.
 - c) Locate the setting that you want to modify.
Note: In a folder with many settings, you might want to increase the items per page. You can also go directly to a selected page.
 - d) Click a setting in the list.
 - e) Make your changes in **Value**.
 - f) Click **Done**.
The change is saved.
3. To add a custom folder, click **New Folder**.
 - a) Enter a **Name**.
The name should begin with a letter and can contain letters, numbers, space, underbar, and hyphen.

- b) Click **Choose** and drill down into **Folder Path** to select where to place the new folder.
- c) Click **Done**.

The folder is added.
4. To add a custom setting, click **New Setting**.
 - a) Enter a **Name**.
 - b) Enter a **Description**.
 - c) Click **Choose** and select a **Folder Path** where the new setting is saved.
 - d) Enter a **Value**.
 - e) Set **Encrypted** to true to make the value of the setting encrypted.
 - f) Click **Add**.

The setting is added.
5. To copy a custom setting or folder:
 - a) Select a setting or folder that you want to copy.
 - b) Click **Copy to**.
 - c) Choose a folder where the new setting or folder belongs.
 - d) Click **Done**.

The setting or folder and all of its settings is copied. You can change the description but not the name of the new setting.
6. To delete a custom folder or setting:
 - a) Select a custom folder or setting that you want to delete.
 - b) Click **Delete**.
 - c) Click **Delete**.

The folder or setting is deleted.

Paths for settings in data loader files

In data loader XML files, the path of a setting begins with `/OpenPages/`. The `OpenPages` folder is hidden in the user interface, but you must include it in the path when you work with settings in a data loader file.

For example, in the user interface, the path to the **Transaction timeout** setting for FastMap is:
Applications > GRCM > FastMap > Transaction timeout.

In a data loader file, the path is `/OpenPages/Applications/GRCM/FastMap/Transaction timeout`. The path is specified in the name attribute of the `<registryEntry>` element. The following example shows the syntax:

```
<registryEntry name="/OpenPages/Applications/GRCM/FastMap/Transaction timeout"
               description="The maximum time in seconds that a process can run for."
               hidden="false"
               encrypted="false"
               protected="true"
               value="41600"/>
```

For more information, see [“Creating a data loader file” on page 732](#).

Applications folder settings

The registry settings in the Application folder represent a select list of individual settings.

All of the following actions are accessed from the Applications folder.

To access the Applications folder, you must have Settings application permission set on your account.

Configure the browser cache

Affect the behavior of the browser's back and forward icons by changing the value of the Disable Browser Cache setting.

Applications > Common > Configuration > Disable Browser Cache

Default: **false**

Values:

- **true** - the browser's cache is disabled; using the back icon sometimes requires a refresh command for the page to display.
- **false** - the browser's cache is enabled and no refresh action is required; however, the data on the page might be whatever was cached in the browser.

Displaying the accessibility link

You can modify the **Help** menu to include a link to an accessibility policy.

About this task

You can add an accessibility link to the **Help** menu. When a user clicks the Accessibility link, a page opens with information about your company's accessibility policy for users with disabilities. The linked page can be to a location on your intranet or to a page you are hosting in OpenPages. The link opens in a new tab.

You define the **Accessibility** menu item by using application text labels and registry settings.

- You define the menu item name in **app.header.accessibility.label**. This name is what users see in the menu. The default is **Accessibility**.
- You define the link in the **Applications > Common > Accessibility > URL** setting. When users click the menu item, this link opens in a new tab.

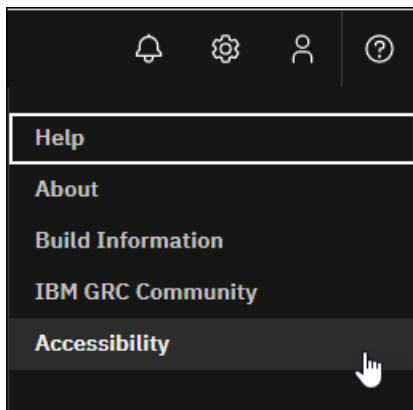


Figure 63. Help menu with the Accessibility menu item

The placement of the **Accessibility** item in the menu is fixed and cannot be changed.

Each locale can have one name for a menu item. The user's locale determines the text that is displayed. The text that is defined in the en_US locale is the default text if the user's locale is not saved in the browser.

Procedure

1. Click > **System Configuration > Application Text**.
2. Click to access the search filter.
3. Click **Labels**.

4. Search for the **Accessibility** menu item, specify the name of the menu item in **app.header.accessibility.label**.
 5. Click the name of the locale code you want to modify.
For example, click **en_US**.
 6. Type the text that you want to display in the menu.
 7. Click **Done**.
 8. To specify to display when users click the accessibility menu item, enter the URL of the accessibility policy page in the **Applications > Common > Accessibility > URL** setting.
- Note:** If you want to host the accessibility policy page on the IBM OpenPages server, perform the following steps:
- Put the accessibility policy HTML file into the <OP_HOME>/wlp-usr/shared/apps/op-apps.ear/taskui.war folder.
 - Enter /<name_of_html_file> in the **Applications > Common > Accessibility > URL**.
9. Refresh the browser page to see your changes.
- Tip:** To remove a menu item, clear the text in its application text label and remove the URL from its registry setting.

Defining the Privacy and Acceptable Use menu items

You can modify the **Help** menu to include links to a privacy statement and an acceptable use policy.

About this task

You can add the following items to the **Help** menu:

- A privacy statement menu item

Opens a link, for example, to an intranet site with more information about privacy. The link opens in a new tab.

- An acceptable use policy menu item

Opens a link, for example, to an intranet site with more information about acceptable use. The link opens in a new tab.

You define a menu item by using application text labels and registry settings.

Privacy Statement menu item

You define the menu item name in **app.header.privacy.label**. This name is what users see in the menu. The default is **Privacy Statement**.

You define the link in the **Applications > Common > Privacy Link URL** setting. When users click the menu item, this link opens in a new tab.

Note: This link is also used by the privacy statement link on the login page. For more information, see [“Defining messages and behavior on the login screens” on page 451](#).

Acceptable Use Policy menu item

You define the menu item text in **app.header.acceptable.use.label**. This name is what users see in the menu. The default is **Acceptable Use Policy**.

You define the link in the **Applications > Common > Acceptable Use URL** setting. When users click the menu item, this link opens in a new tab.

Note: This link is also used by the acceptable use policy link on the login page. For more information, see [“Defining messages and behavior on the login screens” on page 451](#).

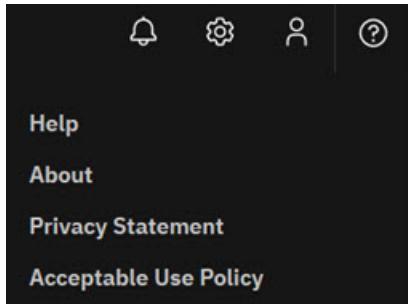


Figure 64. Help menu with the Privacy and Acceptable Use menu items

The placement of the **Privacy Statement** and **Acceptable Use Policy** items in the menu is fixed and cannot be changed.

Each locale can have one name for a menu item. The user's locale determines the text that is displayed. The text that is defined in the en_US locale is the default text if the user's locale is not saved in the browser.

Procedure

1. Click > **System Configuration** > **Application Text**.
2. Click to access the search filter.
3. Click **Labels**.
4. Search for one of the following labels, and then click the link to edit the application text.
 - For the **Privacy Statement** menu item, specify the name of the menu item in **app.header.privacy.label**.
 - For the **Acceptable Use Policy** menu item, specify the name of the menu item in **app.header.acceptable.use.label**
5. Click the name of the locale code you want to modify, for example, en_US.
6. Type the text that you want to display in the menu.
7. Click **Done**.
8. Specify the URL to display when users click the menu items.
 - a) Click > **System Configuration** > **Settings**.
 - b) Edit the following settings:
 - For the **Privacy Statement** menu item, specify the URL of the privacy statement in the **Applications** > **Common** > **Privacy Link URL** setting.
 - For the **Acceptable Use Policy** menu item, specify the URL of the acceptable use policy in the **Applications** > **Common** > **Acceptable Use URL** setting.
9. Log out and log back in to see your changes.

Tip: To remove a menu item, clear the text in its application text label and remove the URL from its registry setting.

Display or hide field guidance

Show or hide field-specific guidance on the an object's Creation, Task, or Admin View through the **Show Field Guidance** setting.

By default, the **Show Field Guidance** setting is set to display in the application. When a user clicks a question mark icon next to a specific field on an object's Creation, Task, or Admin View, the field guidance text is displayed.

Applications > Common > Configuration > Show Field Guidance

Default: true

Values:

- **true** - the question mark icon and field guidance text is displayed to users.
- **false** - the question mark icon and field guidance text is hidden from users.

Display or hide system generated field guidance

The **Show System Generated Field Guidance** setting controls whether information about field dependencies and dependent picklists is appended to field guidance.

For this setting to have effect, the **Show Field Guidance** setting must be set to true. If **Show Field Guidance** is false, then no guidance would be shown in any event. For details, see “[Display or hide field guidance](#)” on page 477.

Applications > Common > Configuration > Show System Generated Field Guidance

Default: true

Values:

- **true** - shows system-generated dependencies information.
- **false** - suppresses system-generated dependencies information.

Disable the New capability from various launch points

You can disable the **New** capability for any or all objects from several launch points within the product. There is a different registry setting for each of the launch points.

These launch points do not prefill parent information. If users find it difficult to select the most appropriate parent information for particular object types, you can disable the **New** capability.

Note: The **Object Types Disabled** setting overrides these settings. If an object type is disabled everywhere, there is no need to disable the New capability individually for each launch point. For more information about the **Object Types Disabled** setting, see “[Controlling the availability of object types with the New button on Grid Views](#)” on page 213.

<i>Table 151. Disabling the New capability</i>	
Setting name	Description
Disable Add New Filtered List View Page Global Launch Points	Controls whether the New button appears on Grid View toolbar. When you disable this launch point, users can still use the New capability on the Task or Admin tab to create child objects.
Disable Add New Home Page Dashboard Launch Points	Controls whether the object type appears on the Object Type list when you add a new panel to the Home page Dashboard and select a New type of widget.

Applications > GRCM > Add New Wizard > Disable Add New Filtered List View Page Global Launch Points

Default: none

Values: In the **Value** box, type the names of the objects that you want to disable. Separate each object type with a comma (,). Use the object names and not the object labels. A value of \$ALL\$ disables the launch point for all object types.

Applications > GRCM > Add New Wizard > Disable Add New Home Page Dashboard Launch Points

Default: none

Values: In the **Value** box, type the names of the objects that you want to disable. Separate each object type with a comma (,). Use the object names and not the object labels. A value of \$ALL\$ disables the launch point for all object types.

Modify the deletion interval for a reporting period

You can configure the number of days in which a reporting period can be deleted after it is created. After the specified interval, the reporting period can no longer be deleted.

Applications > GRCM > Reporting Periods > Delete Interval

Default: 7 days

Value: In the **Value** box, edit the number of days you want for the deletion interval.

Show hidden settings

Some settings are hidden to protect these settings from being modified. To display hidden settings, change the value in the **Show Hidden Settings** setting.

Applications > Common > Configuration

Default: false

Values:

- **true** - show hidden settings.
- **false** - hide hidden settings.

Specify the browsers that can access IBM OpenPages

You can specify which browsers can be used to access IBM OpenPages with Watson by configuring a list of allowable browsers. All browsers that are not in the list are blocked.

To use the **Allowed Browsers** setting, do the following steps:

1. Ensure that the following settings are enabled (set to true):
 - Platform > Security > Cross-site Scripting Filter
 - Platform > Security > Advanced XSS Filter
2. Configure the **Allowed Browsers** setting. For more information, see [“Allowed Browsers setting” on page 479](#).
3. Add the following environment property to the <OP_HOME>/aurora/conf/aurora.properties file.

```
enforce.browser.support=true
```

4. Restart the OpenPages application servers.

To disable this feature, set the `enforce.browser.support` environment property to `false` and then restart the OpenPages application servers.

Allowed Browsers setting

Applications > Common > Configuration > Allowed Browsers

Default: Empty, all browsers are allowed to access OpenPages

Values: A list of allowed browsers.

Type a pipe (|) delimited list of browsers that users can use to access OpenPages. The delimited list can specify browsers in general or specific versions of a particular browser.

To allow Microsoft Edge Chromium, type Edg (without the e on the end).

To specify a particular browser version, you need to know the User-Agent value for the browser that you want to add to the list. For example, for Microsoft browsers, see <https://docs.microsoft.com/en-us/microsoft-edge/web-platform/user-agent-string>.

Example: Allow Microsoft Edge Chromium and Google Chrome.

Edg | Chrome

User provisioning settings

Administrators can configure the behavior of the Create User wizard and the Users page with the following settings.

To access the user provisioning settings menu items, you must have the Settings application permission set on your account.

Copy Access From Inactive

Determines whether inactive users can be the source for the **Copy Access From** operation.

Applications > Common > Administration > User Provisioning > Copy Access From Inactive

Default: true

Values:

- true - allows you to select inactive users to copy access from.
- false - inactive users cannot be selected to copy access from.

Copy User Info Attributes

Determines the default behavior for the Locale, Profiles, Group Memberships, Direct Role Assignments, and Direct Reports Access attributes during the Copy Access From operation. A name=value pair is used for each attribute, such as Locale=Yes. Name=value pairs are separated by a comma.

Applications > Common > Administration > User Provisioning > Copy User Info Attributes

Default: Locale=Yes,Profiles=Yes,Group Memberships=Yes,Direct Role Assignments=Yes,Direct Reports Access=Yes

Values: If a name pair is missing, the copy operation is not available. For example, if Profiles=Yes is not listed in the **Value** box, profiles are not copied during the copy operation.

- Yes - by default, the attribute is copied.
- No - by default, the attribute is not copied. If a name=value pair is missing, No is assumed. For example, if Profiles=Yes is not listed in the Value box, profiles are not copied by the copy operation.
- Not available - the attribute cannot be copied.
- blank - if the **Value** box is empty, the Copy Access From operation is not available.

Copy User Info Choice

Determines whether the Copy Access From operation adds to or replaces a user or group's existing attributes.

Applications > Common > Administration > User Provisioning > Copy User Info Choice

Default: Replace

Values:

- Replace - existing attributes are overwritten by the Copy Access From operation.
- Add - new attributes are merged with existing ones and duplicates are removed. No validation is done after the merge to ensure that there are no conflicts.
- Choice - means you can choose between Add or Replace each time that you do a Copy Access From operation.

- **Not Available** - you cannot perform the Copy Access From operation.

Default Allowed Profiles

Determines the default value or values for the Allowed Profiles.

Applications > Common > Administration > User Provisioning > Default Allowed Profiles

Default: blank

Values: Possible values are any profiles in the system. Use a dollar sign and semicolon (\$) to separate profile names in the list. If the value is blank, the Default Profile is used as the Allowed Profile.

Note: Disabled profiles cannot be used as an Allowed Profile, even if they are included in this list.

Default User Change Password

Determines the default change password behavior when you create a new user.

Applications > Common > Administration > User Provisioning > Default User Change Password

Default: blank

Values:

- blank - if the **Value** box is empty, the password expires in 90 days, and the user can change the password then.
- **cannot** - user cannot change password. Using this value forces **Password never expires**, and ignore the **Default User Password Expiration** setting.
- **must** - user must change password at next logon.

Default User Password Expiration

Determines the default password expiration behavior.

Applications > Common > Administration > User Provisioning > Default User Password Expiration

Default: blank

Values:

- blank - password expires in 90 days.
- *n* - password expires in *n* days, where *n* is an integer in the range 1 - 9999.
- **never** - password never expires

New User Default Locale

Determines the default value for the locale.

Applications > Common > Administration > User Provisioning > New User Default Locale

Default: en_US

Values: Allowed values are any of the OpenPages supported locale codes, such as de_DE, en_US, and it_IT.

Reports Access Page Size

Determines the number of rows that are listed per page in the Reports Access table.

Applications > Common > Administration > User Provisioning > Reports Access Page Size

Default: 20

Values: In the **Value** box, type a positive integer. If the number of rows is less than this number, there is no paging.

Users Can Copy Access From

Determines which users can be used as source for the Copy Access From operation.

Applications > Common > Administration > User Provisioning > Users Can Copy Access From

Default: blank

Values: In the **Value** field, type a comma-separated list of users that can be used as source for the Copy Access From operation. If the value is blank, no users can be used as source for the copy operation. A value of **\$ALL\$** means that any user can be used as source. Use the **Copy Access From Inactive** setting to determine whether inactive users can be used. For more information, see “[Copy Access From Inactive](#)” on page 480.

Actor selectors: Configure the bucket size of the phonebook

You can use the **Bucket Size** setting to control the number of user names that are displayed in a bucket or category within the User Selector phonebook style pop-up dialog box.

The number of buckets that are displayed in the phonebook is determined by the size of the bucket and the number of users. For example, if there are 100 users and the bucket size is set to 20, the phonebook would display 5 buckets of 20 users per bucket.

Applications > Common > User Selector > Bucket Size

Default: 10

Values: In the **Value** box, type a numeric value for the number of users you want displayed per bucket.

Menus: Modify the order of menus

The Primary menu (☰) in IBM OpenPages with Watson contains various menus that represent categories for grouping object types. Use the **Items** setting to modify the order in which the menus are displayed.

Which categories for object types are available as menus depends on your particular business solution.

Applications > GRCM > NavigationMenu > Items

Values: In the **Value** box, modify the order of the menus as you want these to appear in the Primary menu.

Note:

- The list must be comma delimited.
- The order in which the menus are defined in the list determines the order in which the menus are displayed in the application user interface.

In the following example, the menus are displayed as follows: **Organization**, **Remediation**, and then **Audit Management**.

Organization,Remediation,AuditManagement

- The list must not have any leading or trailing spaces.

Changes to menus do not appear until users log out and then log back in to the application.

Menus: Modify submenus

IBM OpenPages with Watson displays menus that represent categories for grouping views and object types.

Applications > GRCM > NavigationMenu > <folder_name>

Default: none

Values:

Note:

- The list of menu items must be comma delimited.

- The order in which the menu items are defined in the list determines the order in which the items are displayed in the selected menu on the application user interface.
- The list must not have any leading or trailing spaces.

Object auto-naming settings

For most object types, you can auto-generate their names when they are created or copied. This ability allows users to enforce internal naming policies and ensure unique object names.

The auto-generation of object names is controlled by a series of settings. It is possible to turn autonaming on or off for each object type individually. For example, you might want all business entities and processes to be named by users, but all risks, controls, and test plans named automatically by the IBM OpenPages with Watson application.

Note: Auto-naming is not supported for the following object types: SOXDocument and SOXSignature.

Although auto-naming is not supported for SOXDocument objects, you can control how duplicate file names are handled. For information, see [“SOXDocument object auto-naming settings for duplicate file names” on page 485](#).

Applications > GRCM > Auto Naming

Default: none

Values: For each object type, you can modify the following settings:

Table 152. Auto-naming settings to modify	
Setting name	Description
Auto-named folder	Flags this folder as using auto-naming.
New object	Determines whether new instances of the object are automatically named. If the value is set to: <ul style="list-style-type: none"> • true - auto-naming is enabled for new instances. • false - auto-naming is disabled for new instances. The default value is false .
Can be edited	Determines whether the generated name can be edited during the creation process. If the value is set to: <ul style="list-style-type: none"> • true - the generated name can be edited. • false - the generated name cannot be edited. The default value depends on the object type.
Default parent name	If the created object has no parent, the value for this parameter will be used to replace the "%P;" variable in the generated name.
Format	Determines the format of the generated name. Additional details can be found in “Configure the format of object names” on page 483 .

Configure the format of object names

The **Format** setting allows you to incorporate some contextual information about the object, as well as an identifier in the object name.

You can use the variables that are described in the following table to format the auto-generated name.

Applications > GRCM > Auto Naming > <object_type> > Format

Default: none

Values:

- In addition to the variables, you can include any valid text in the auto name.
- The name of an object:
 - Must be 252 bytes or less.
 - Cannot contain forward slashes (/), backslashes (\), or the ellipsis character (...).
 - Must contain either the %Nn ; or the %Rn ; token.

Table 153. Auto-naming variables

Variable	Meaning
%P ;	Will be replaced with the name of the parent of the new object. If the created object has no parent, the value of the default setting will be used.
%U ;	Will be replaced with the creator's user name.
%Nn ;	A unique sequentially generated numeric identifier. Where n specifies the amount of padding the number has. For example, %N3 ; might result in 001, 002, 003, while %N5 ; might result in 00001, 00002, 00003, and so forth.
%Rn ;	A unique randomly generated alphanumeric identifier. The identifier uses A-Z, a-z, and 0-9. Where n specifies the amount of padding the number has. For example, %R3 ; might result in T6d, while %N5 ; might result in T6d3ff, and so forth.

Name examples

For the following examples, suppose you have a parent Process that is called Hiring Practices with child Risks, a creator of JSmith, and the following settings for Risks:

- **Auto-Named** value is set to **true**
- **Can be Edited** value is set to **false**
- **Format** value is set to **%P;_RIS_%N7;**
- **Default Parent Name** has no value set.

The auto-generated name is Hiring Practices_RIS_0000001 and cannot be edited.

Example 1:

If you change the auto-naming **Format** to **%P;-Risk-%N5;**, the generated Risk name is Hiring Practices-Risk-00001.

Example 2:

If you change the **Format** parameter to **Risk %N3; for %P; (%U;)**

The generated name is Risk 001 for Hiring Practices (JSmith).

Example 3:

You don't need to use all of the variables in an auto-generated name. For example, you can set **Format** to **Risk %N4;**.

The generated name is Risk 0001.

Example 4:

If the risk has no parent process, the value of **Default Parent Name** is used. For example, if you set **Format** to %P ; _RIS_%N7 ;, the generated name is _RIS_0000001.

SOXDocument object auto-naming settings for duplicate file names

Use the Auto Remediate Duplicate File Names setting to control auto-naming for SOXDocument objects.

Within a folder, file names for SOXDocument objects must be unique. This setting controls what happens when a duplicate file name is added. The system can add a numeric suffix to the file name or force the user to rename it.

Applications > GRCM > Auto Naming > SOXDocument > Auto Remediate Duplicate File Names

Default: true

Values:

- **true** - adds a numeric suffix to the file name.
- **false** - forces users to rename the file.

In questionnaire assessments and IBM OpenPages Loss Event Entry, this setting is ignored and duplicate file names are automatically renamed.

Environment migration settings

If your organization has multiple IBM OpenPages with Watson environments, you can move data from one environment to another without needing physical access to either environment. Migration means exporting from a source environment and importing into a target environment. You can use settings to configure the environment migration tools.

Applications > GRCM > Environment Migration

For more information, see ["Settings that apply to environment migration" on page 719](#).

Report fragment settings

For all profiles, you can globally configure the size of the pop-up window for report fragment fields in certain object views.

A report fragment pop-up window can be sized:

- Manually - by specifying the size of the pop-up on the field definition page of a report fragment field.
- Automatically - if no size is specified on the field definition page of a report fragment field, the pop-up window will be automatically sized using the settings in [Table 154 on page 485](#).

For report fragment fields with a display type of 'Automatic', the display behavior varies depending on the object view:

- For Task View pages - Cognos report components are always embedded directly into the cell of the report fragment field.
- For Grid View - Cognos report components are displayed in pop-up windows.

Applications > Common > Report Fragments > Popup

Values: Click one of the settings. In the **Value** box for the selected setting, change the existing value to a new number greater than zero.

Table 154. Settings for reporting fragment pop-up windows

Setting	Description	Default Value
Maximum Height	Sets the default maximum height allowable for a report fragment pop-up window.	375

Table 154. Settings for reporting fragment pop-up windows (continued)

Setting	Description	Default Value
Maximum Width	Sets the default maximum width allowable for a report fragment pop-up window.	575
Minimum Height	Sets the default minimum height allowable for a report fragment pop-up window.	250
Minimum Width	Sets the default minimum width allowable for a report fragment pop-up window.	350

Configuring your mail server

Configure your mail server so you can automatically send email notifications to users.

- The mail server settings are used for mail routing for objects that use workflows, such as questionnaire assessments and incidents, and for objects that use lifecycles. Email notifications are sent to assignees when a workflow or lifecycle starts and for each transition except for close transitions.
- The **Mail Server** setting is used to configure your mail server so you can automatically send email notifications to users from your JSP-based reports or the Notification Manager utility.

For emails generated by workflows, the sender address is specified in **Applications > Common > Email > Mail From Address**. The default is donotreply@openpages.com. You can also set the sender name in **Applications > Common > Email > Mail From Name**. For more information about workflows, see [Chapter 16, “Configuring GRC Workflow,” on page 369](#).

For emails generated by lifecycle triggers, the sender address is specified in the `trigger.xml` file. The default is donotreply@openpages.com. For more information about lifecycle triggers, see the *IBM OpenPages with Watson Solutions Guide*.

Settings

Depending on your environment, you can configure the following settings:

- SMTP Password**
- SMTP Port**
- SMTP Security Type**
- SMTP User Name**
- SOCKS Proxy Private IP Address**

Some settings might be hidden. For more information about unhiding settings, see [“Show hidden settings” on page 479](#).

Define **SMTP Port** and **SMTP Security Type** if you use a third-party SMTP provider. Valid values for **SMTP Security Type** are SSL/TLS and STARTTLS. You must also import the SSL certificate from the SMTP server provider. Refer to the SMTP provider's documentation and import it by using `keytool`. Leave **SMTP Port** and **SMTP Security Type** empty if you have an unencrypted connection that uses the default port number. In this case, the SMTP servers are behind a firewall and a third-party SMTP provider is typically not used.

Note: You can override this global setting by entering the name of a mail server in the notification Mail Server parameter.

Applications > Common > Email

Default: mail.yourcompany.com

Values: In the **Value** box, enter the values for **Mail Server**, **SMTP Password**, **SMTP User Name**, and **SOCKS Proxy Private IP Address**, as required by your mail system.

In **Mail Server** enter a fully qualified server hostname, for example, `mail.openpages.com`.

This video demonstrates how to configure your email server for notifications:

<https://youtu.be/0lbJtoCogSw>

Date field display format

The **Date field display format** setting controls how date fields are displayed for GRC objects. It does not affect dates that appear in other areas of the system. It affects only how date fields are displayed and not the format when users enter date values.

The **Date field display format** setting and the locale determine how date fields are displayed. The examples below illustrate how the date, October 25, 2016, is displayed given different date formats and locales:

<i>Table 155. Date field display format</i>		
Locale	Date field display format	Result
US English	SHORT	10/25/16
US English	MEDIUM	Oct 25, 2016
US English	LONG	October 25, 2016
UK English	SHORT	25/10/16
UK English	MEDIUM	25-Oct-2016
UK English	LONG	25 October 2016
Simplified Chinese	SHORT	16-10-25
Simplified Chinese	MEDIUM	2016-10-25
Simplified Chinese	LONG	2016年10月25日

Applications > GRCM > Date Field Display Format

Default:

The values are:

- **short** - dates are displayed in Java Locale SHORT format.
- **medium** - dates are displayed in Java Locale MEDIUM format.
- **long** - dates are displayed in Java Locale LONG format.

Configuring large files for upload

By default, the maximum upload size for files in IBM OpenPages with Watson is 250 MB. If you have files that are larger than this limit, you can configure the system to upload larger files. Files greater than 2 GB are not supported.

Procedure

1. Log on as a user with administrative privileges.
2. Click  > **System Configuration** > **Settings**.
3. Click **Applications > Common > Max File Upload Size**
4. In the **Value** field, type the maximum upload size as a numeric value followed by a single letter to represent the unit. For example: 200K, 500M or 1G.
5. Click **Done**.
6. Restart the OpenPages with Watson application service.

For details on starting services, see Chapter 25, “Starting and stopping servers,” on page 709.

Enabling and configuring the opening of Microsoft Office files

You can configure whether users can open and edit Microsoft Office files directly from OpenPages.

Before you begin

Verify that Microsoft Office 2016 or Microsoft 365 is installed locally for users.

Verify that SSL is enabled.

Test that users can open Microsoft Office files from OpenPages.

If the OpenPages application server is using a self-signed certificate, users must import the certificate into the truststore on their local computer. Otherwise, a blank screen is displayed when they try to open a Microsoft Office document from within OpenPages. This type of certificate might be used in certain situations, for example, in a test environment.

1. Click the lock icon in the browser URL (Chrome).
2. Click **Certificate**.
3. Click the **Details** tab and click **Copy to File** to export the certificate.
4. Click **Next** and accept all defaults.
5. Enter a file name and click **Finish**.
6. From the Control Panel, type **Manage User certificates** to open the certmgr tool.
7. Click **Trusted Root Certificates > All Tasks > Import** to import the certificate you saved.
8. Close the browser.
9. Open a new browser session.

About this task

How this feature works is similar to inline editing. Users can open Microsoft Office files directly from OpenPages. Every time a user clicks save within a file that is opened in this way, the file is saved in the OpenPages file repository. However, other users cannot see the changes until the file is checked in.

If enabled, users can open Microsoft Office files in the following places in the OpenPages UI:

- In a Task or Admin View for an object type, where the view contains a Grid relationship field for the File object type.
- In a Task or Admin View for the File object type, in the **Versions** section.

The feature is available:

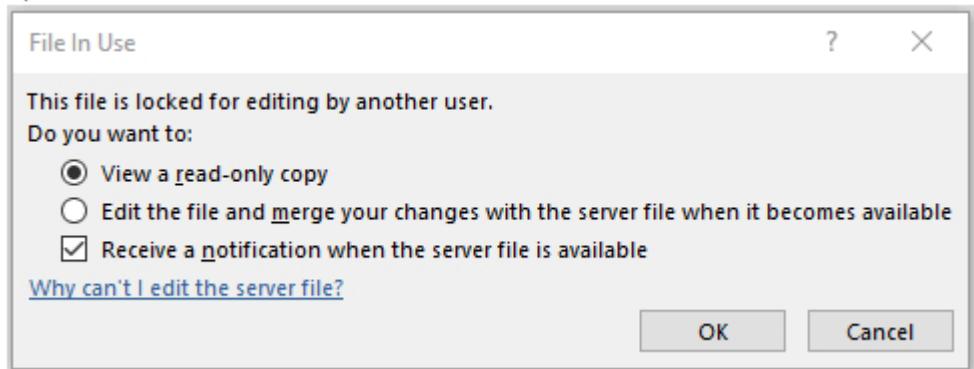
- Only on Microsoft Windows clients. It is not available on Mac operating systems.
- Only if Microsoft Office 2016 or Microsoft 365 is installed locally for users.
- Only for Word, Excel, and PowerPoint files with the following extensions: .doc, .docx, .xls, .xlsx, ppt, .pptx. This feature is not available for other file types, such as PDF files and text files.
- Only if the OpenPages URL has an HTTPS protocol, not HTTP.

The following settings are already set to the recommended defaults, but administrators can decide to change them to preserve the behavior of previous versions:

- Deciding whether to display the **View** button

The **View** button is no longer displayed by default. The **View** button provides a user the ability to view the file if another user has it checked out. It is not to be used to edit the file because the user would get no reminder about checking the file back in. However, the user can choose to edit the file after clicking the **View** button. This action can lead to a situation where the user tries to edit a file while another user

is editing the file, and there is no easy way to resolve the conflicts. The Microsoft application displays a dialog box with some options, but only **View a read-only copy** works.



Without the **View** button, if a user wants to look at the file while another user has the file checked out, the user downloads the file and opens it manually. If the user wants to just look at the file and not edit it, they can click the **Edit** button and then either cancel the checkout or check in the file when they are done.

If you want to display the **View** button, ensure that all users know to select only the **View a read-only copy** option in the Microsoft application **File In Use** dialog box.

To display the **View** button, click **Applications > Common > Configuration > MS Office desktop > Show View button** and set the **Value** to **true**.

- Deciding when the file gets checked out

By default, a file is checked out as soon as the user clicks the **Edit** button. Checking out the file immediately prevents other users from trying to edit the file. However, the file always gets checked out, even if the user never edits it. If the user doesn't edit the file, the user must manually undo the checkout.

If you want to restore the behavior from pre-8.3.0.2 releases, you can do so. In the past, the default behavior was to delay the check out until the user clicks **Enable Editing** and automatically cancel the check out if the user closes the document with no changes. If you choose to restore this behavior, ensure that all users know to select only the **View a read-only copy** option in the Microsoft application **File In Use** dialog box.

To restore the checkout behavior from versions before 8.3.0.2, set **Applications > Common > Configuration > MS Office desktop > Checkout immediately on edit** to **false**.

View and **Edit** are displayed in Task and Admin Views if the following conditions are met:

- The application setting **Applications > Common > Configuration > Disable opening files with MS Office desktop** is set to **false**. This setting is the default.
- View** is displayed if the user has read access rights to the file and the application setting **Applications > Common > Configuration > MS Office desktop > Show View button** is set to **true**.
- Edit** is displayed if the user has write access rights to the file and if no other users have the file checked out.

Procedure

- Log on as a user with administrative privileges.
- Click > **System Configuration > Settings**.
- Click **Applications > Common > Configuration > Disable opening files with MS Office desktop**.

In the **Value** field, type a value:

- false** - editing is enabled so that users can open and edit Microsoft Office files directly from OpenPages. This setting is the default.

- **true** - editing is disabled so that users cannot open and edit Microsoft Office files directly from OpenPages.

Click **Done**.

Reviewing the Net Promoter Score (NPS) survey settings

The **Applications > NPS > Embedded Survey URLs** setting is part of the integration between a Net Promoter Score survey provider and OpenPages.

About this task

OpenPages provides a default URL value that should not be changed except on the advice of IBM OpenPages Support.

Procedure

1. Log on as a user with administrative privileges.
2. Click  > **System Configuration** > **Settings**.
3. Click **Applications > NPS > Embedded Survey URLs**.
4. In the **Value** field, review the URL of the embedded NPS survey provider.
5. Click **Done**.

What to do next

Complete the remaining steps to configure a Net Promoter Score survey. For more information, see “Configuring a Net Promoter Score survey” on page 239.

Signature and lock settings

IBM OpenPages with Watson allows users to create "signatures" on objects. A signature is a note that signifies the user agreement that the object meets with the user approval. It has no enforcement powers, and does not prevent the item from being modified after approval is given.

A signature lock is a lock that is placed on an object and its descendants. It prevents the objects from being modified. The lock is activated by placing a signature on an object. After the signature is added, the lock is active. The signed object and all of its associated child objects in the object hierarchy cannot be modified until an administrator removes the lock.

Only one active lock can be placed on an object. Multiple locks can be inherited from parent objects as those objects are locked.

All of the following actions are accessed from the Applications folder.

To access the registry settings, you must have the Settings application permission set on your account.

Configure signatures

When you add a group to an object type setting for signatures, sign off is enabled for objects of that type. Users who belong to the group can add and revoke signatures.

Note: Only groups that are defined in object type can sign off on objects of that type. Subgroups of a group do not inherit the sign-off permission.

Applications > GRCM > Signature > Permission > <object_type>

where <object_type> is the object type of the object you want to enable for sign off

Values: In the **Value** box, complete the following steps:

- To configure groups to add a signature to the object type, type the name of the group to add.

Note: If you are entering multiple user groups, use a comma to separate group names, and do not use a space after the comma.

For example, to add the Auditors and Managers groups to the sign-off list for Process object types, the value in the SOXProcess setting is defined as follows: **Auditors,Managers**

- To disable one or more user groups from adding a signature to the selected object type, delete the group name.

Configure signature locks

The **Mode** setting controls whether a lock is created when a signature is added. When the Autolock value is set, adding a signature to an object creates a lock on the object. It prevents further changes to the object and any object that is associated with it. Revoking a signature removes the associated lock.

Note: When the locking feature is enabled, users can create signatures only on items to which they have Write privileges.

Applications > GRCM > Signature > Mode

Default: none

Values: In the **Value** field, type one of the following values:

Table 156. Lock values

Value	Action
None	No lock is applied to the object when a signature is added.
Autolock	The object is locked when a signature is added. Only users with Write permission for an object can create a signature.
Cascade	Cascading signatures as specified in the Cascade setting are enabled for child objects (for details see, “Configure signatures” on page 490).

Configure the signature status field

The OPSS-Sig:Status field contains enumerated values for signature status.

About this task

The OPSS-Sig:Status field is by default a single-value enumerated field with two values: *In Effect* or *Revoked*.

An issue exists in that if you change OPSS-Sig:Status to a multi-valued enumerated field, signatures can no longer be created.

A workaround for this issue is to set the **Applications > GRCM > Special Object Fields > SOXSignature Status Field** registry setting to OPSS-Sig.Status.In Effect.

When **Applications > GRCM > Special Object Fields > SOXSignature Status Field** is set to OPSS-Sig.Status.In Effect, signatures can be created. Signatures can also be revoked but only when a Chrome browser is used.

Configure cascading signatures

When a signature is added to a parent object, you can automatically apply signatures to all associated objects in the hierarchy, below the signed object. For example, signing a process applies the signature to any sub processes, accounts, risks, controls, and tests that are associated with the process.

This feature is turned off by default. It is enabled through the **Cascade** setting.

Note: To enable cascading signatures, the **Mode** setting must have the **Cascade** value set (for details see, “Configure signature locks” on page 491).

Applications > GRCM > Signature > Cascade > <object>

Default: none

Values: In the **Value** box, complete the following steps:

- To add a cascading signature to child objects, type the name of the child object type.

Note: If you are entering multiple child objects, use a comma to separate the names, and do not use a space after the comma.

For example, to add a cascading signature to the Process object type for child subprocesses, accounts, and risks, the value in the SOXProcess is set to the following value:

SOXSubprocess,SOXAccount,SOXRisk

- To remove a cascading signature from child objects, delete the name of the child object type.

Lock and unlock objects

Locks can be applied to objects without the use of signatures.

Users lock entire object hierarchies by adding a signature, if Autolock is enabled, or by clicking the **Lock**

 **Resource** icon on an object.

The **Lock** and **Unlock** application permissions control whether users can lock and unlock objects. For details, see “Configure the Lock and Unlock application permissions ” on page 492.

Note: Unlocking an object using the **Actions > Unlock this** menu item does NOT revoke the signature.

Access privileges for locking

By default, "Read" permission is required to lock an object. This setting can now be configured through a property in the *aurora.properties* file named "allow.locking.read.access". This property is set to false by default.

When set to 'true', users with Read access to an object can lock the object by adding a signature. The default value of false requires that users have at least "Write" access to an object before they are allowed to lock it.

Configure the Lock and Unlock application permissions

The **Lock** and **Unlock** application permissions control whether users can lock and unlock objects.

The **Lock** application permission allows a user to lock any unlocked object, as long as the user has Write permission to the object and all associated objects down the hierarchy.

The **Unlock** application permission allows a user to unlock any locked object, as long as the user has Write permission to the object and all associated objects down the hierarchy.

You assign application permissions either to a role template or to a user group that a user belongs to.

- On a role template, the **Lock** and **Unlock** application permissions are defined in:
 - **Administration > Role Template > <role template> > Role Permissions > Files > Lock**
 - **Administration > Role Template > <role template> > Role Permissions > Files > Unlock**
- On a user group, the **Lock** and **Unlock** application permissions are defined in:
 - **Administration > Users, Groups and Domains > <group> > Permissions > Files > Lock**
 - **Administration > Users, Groups and Domains > <group> > Permissions > Files > Unlock**

For more information, see “Defining application permissions” on page 51.

Configure the lock icons for object types

The **Display Lock Button** setting controls by object type whether lock/unlock icons are displayed.

The **Display Lock Button** setting controls whether the lock and unlock icons are displayed for an object type. The user must be assigned the **Lock** application permission for the lock icon to display. The user must be assigned the **Unlock** application permission for the unlock icon to display.

The **Display Lock Button** setting does not control the object types that may be locked by a workflow action. When a object is locked by a workflow action and the object type is not included in the **Display Lock Button** setting, the lock icon is displayed but a user is unable to unlock the record from a task view or grid view unless the object type is included within the setting.

For more information about lock and unlock application permissions, see [“Configure the Lock and Unlock application permissions” on page 492](#).

Applications > GRCM > Locks > Display Lock Button

Default: none

Values:

- To add an object type, type the name of the object type that is separated by a comma. For example: SOXBusEntity, SOXAccount, SOXSubaccount, SOXProcess, SOXSubprocess, SOXControlObjective, SOXRisk, SOXControl, SOXTest, SOXTestResult, SOXSignature, SOXIissue, SOXTTask, SOXDocument, SOXExternalDocument.
- To remove an object type, delete the name of the object type from the list.

Lock child objects when a parent is locked

You can use the object type settings under the **Lock Child Types** folder to configure locks on child objects when a parent object is locked.

Applications > GRCM > Locked Objects > Lock Child Types

Default: none

Values: In the **Value** box of the selected setting, enter the exact name of one or more child object types that should be locked when the parent object is locked.

Find the exact object name listed under the **Allowed Associations** folder.

Note: If there are multiple child object types, you must add a comma to separate each object name. For example: SOXProcess, SOXControl, SOXIissue, SOXDocument, SOXExternalDocument, SOXSignature

Configure the registry to enable associations of child objects with locked parents

You can make objects available to users for association when a parent object is locked.

For child object types that are defined in the **Allowed Associations** setting, the **New**, **Add**, **Copy Recursive**, and **Remove** actions are enabled. The **Delete** action is not enabled. For object types that are not defined in the **Allowed Associations** setting, the **New**, **Add**, **Copy Recursive**, **Remove**, and **Delete** actions are disabled when the parent object is locked.

Applications > GRCM > Locked Objects > Allowed Associations > <parent_object_type>

Default: none

Values: In the **Value** field, type the exact name of one or more child object types.

Find the object name listed under the **Allowed Associations** folder (for example, SOXBusEntity).

Note: If you have multiple object types, add a comma to separate each object type name.

For example, by adding SOXProcess and LossEvent in the **Value** field for the **Allowable Associations** folder SOXBusEntity, the **New**, **Add**, **Copy Recursive**, and **Remove** actions are permitted for Process and Loss Event objects associated to a locked Business Entity. These actions will be disabled for any child object of a Business Entity not listed within the **Value** field.

Object Reset settings

Before performing an object reset, you can set the logging level, whether the Reset session should continue or halt if errors are encountered, if ACLs should be checked, and if locks are ignored. These settings need to be set only once, before your first time initiating an object reset, but you may want to change them for different entity trees or ruleset behavior.

Changing the logging level

The **Logging Level** setting controls how much information is displayed on the user interface. The session log captures detailed information regardless of the user interface display setting. You can change the logging information that is displayed on the user interface for a reporting period.

Applications > Common > Object Reset > Logging Level

Default: high

Values:

- low - Only error messages are displayed.
- medium - Both error and warning messages are displayed.
- high - Errors, warnings, and informational or diagnostic messages are displayed.

Continuing on error

The **Continue on Error** setting determines whether the object reset session will log errors and continue to run, or whether the errors will be logged and the session halted. You can change whether the object reset session runs or halts processing when an error is encountered.

Applications > Common > Object Reset > Continue on Error

Default: true

Values:

- true - Errors are logged and processing continues.
- false - Errors are logged and processing is halted.

Obeying ACL restrictions

The **Check ACL** setting controls whether the object reset occurs against all objects contained within the scope of the reset session, or whether the object reset occurs against only those objects to which the user who initiated the reset has access. You can change the scope of the object reset session.

Applications > Common > Object Reset > Check ACL

Default: true

Values:

- true - Includes all objects within the scope of the reset session.
- false - Includes only those objects within the reset session to which the user has access.

Obeying locking restrictions

The **Ignore Locks** setting controls whether existing locks on objects are honored or ignored when running an object reset. You can change whether locks are ignored during an object reset session.

Applications > Common > Object Reset > Ignore Locks

Default: false

Values:

- true - Locks on objects will be ignored when running the reset session.
- false - Locked objects will not be modified by the reset session.

View settings

You can globally configure the following View page settings.



Attention: If you create a new filter that uses the character % as the value, for example Name Contains %2, the Name Contains value field appears empty after you load the filter: the % character does not appear. However, the filter runs properly.

Note: If you are using the FastMap tool, you can also configure FastMap import settings to optimize performance. See “[Modifying export settings to optimize FastMap performance](#)” on page 795 and “[Limiting the rows for import to optimize FastMap performance](#)” on page 795.

Maximum number of objects to export to Microsoft Excel from Grid Views

Use the **Maximum Export Size** setting to control the maximum number of objects that can be retrieved and exported to Microsoft Excel (in .xlsx format) from a Grid View.

If the number of objects that are being exported exceeds the defined number, then the user is prompted to refine their filter.

Applications > GRCM > Filtered List > Maximum Export Size

Default: 1000

Values: In the **Value** field, type a number greater than zero.

Hiding the Export button in Grid Views for profiles

Use the **Export Disabled Profiles** setting to hide the **Export** button in Grid Views, based on the user's current profile.

Applications > GRCM > Filtered List > Export Disabled Profiles

Default: blank

Values: In the **Value** field, type a comma-separated list of profile names. For example, to hide the **Export** button for users with the VRM Vendor and VRM Vendor Manager profiles, type: VRM Vendor,VRM Vendor Manager.

To hide the **Export** button for all profiles, type \$ALL\$.

For example, suppose that you exclude VRM Vendor. When a user who is using the VRM Vendor profile opens a Grid View, the **Export** button is not displayed on the toolbar.

Hiding the Export button in Grid Views for object types

Use the **Export Disabled Object Types** setting to hide or show the **Export** button in Grid Views.

Applications > GRCM > Filtered List > Export Disabled Object Types

Default: blank

Values: In the **Value** field, type a comma-separated list of object type names. For example, if you want to hide the **Export** button in the grid views for Risk and Control object types, type: SOXRisk,SOXControl.

To hide the **Export** button for all object types, type \$ALL\$.

Exclude object types from export

Use the **Object Types to Exclude in Export** setting to exclude object types from exports.

Applications > GRCM > Filtered List > Object Types to Exclude in Export

Default: SOXSignature

Values: In the **Value** field, type a comma-separated list of object type names. For example, if you want to exclude Risk and Control object types from the **Export** dialog box, type: SOXRisk, SOXControl.

Disable Bulk Update link

This setting hides the **Bulk Update** link on the bulk update toolbar in Grid Views.

If **Bulk Update Disabled in Task Focused UI** is set to false, other settings can be used to further refine the feature. For more information, see [“Exclude object types from bulk updates” on page 496](#) and [“Hide the Bulk Update feature for user profiles” on page 496](#).

Applications > GRCM > Filtered List > Bulk Update Disabled in Task Focused UI

Default: false

Values:

- true - the **Bulk Update** link on the bulk update toolbar in Grid Views is not displayed
- false - the **Bulk Update** link on the bulk update toolbar in Grid Views is displayed

Exclude object types from bulk updates

Use the **Bulk Update Disabled Object Types** setting to exclude object types from bulk updates. Use this setting to prevent users from updating information in multiple objects.

This setting hides the **Bulk Update** link on the bulk update toolbar in Grid Views by object type. Another setting controls overall functionality. For more information, see [“Disable Bulk Update link” on page 496](#).

Applications > GRCM > Filtered List > Bulk Update Disabled Object Types

Default: blank

Values: In the **Value** field, type a comma-separated list of object type names that you want to exclude. For example, if you want to exclude Risk and Control object types, type: SOXRisk, SOXControl.

To exclude all object types, type \$ALL\$.

Hide the Bulk Update feature for user profiles

Use the **Bulk Update Disabled Profiles** setting to hide the Bulk Update feature, based on the user's current profile.

This setting hides the **Bulk Update** link on the bulk update toolbar in Grid Views by profile. Another setting controls overall functionality. For more information, see [“Disable Bulk Update link” on page 496](#).

Applications > GRCM > Filtered List > Bulk Update Disabled Profiles

Default: blank

Values: In the **Value** field, type a comma-separated list of profile names that you want to prevent from updating objects in bulk. For example, to hide the Bulk Update feature for users with the VRM Vendor and VRM Vendor Manager profiles, type: VRM Vendor, VRM Vendor Manager.

To hide the Bulk Update feature for all profiles, type \$ALL\$.

Number of levels of object types to export

Use the **Number of Levels to Export** setting to define how many total levels of object types the user can choose to export, including the top-level object that is exported.

This setting is useful for limiting the growth of the tree of objects that a user can export. The number of records that are exported grows exponentially as a user selects more object types to export. For example, if a user selects a single object type, such as Process, and chooses to export its Risks, the Controls under Risks, the Test Plans under Controls and the Test Results under Test Plans, it might result in hundreds or thousands of exported records. Unless the number of levels is limited, the export might take a long time, and might impact system performance for other users.

This setting is hidden by default. For information about unhiding settings, see [“Show hidden settings” on page 479](#).

Applications > GRCM > Filtered List > Number of Levels to Export

Default: View+3

Values: Possible values are View, View+1, View+2, View+3, View+4, View+5.

The maximum value that is respected is View+5.

For example:

- If a user's Grid View is Process - Risk - Control, and this value is **View**, they can export Processes, their Risks, and their Controls. If this value is **View+1**, the user can export Processes, their Risks, and their Controls, and one more object type that is a direct child of Controls. If this value is **View+2**, the user can export one more object type that is a direct child of the first additional object type chosen. If this value is **View+3**, the user can export one more object type that is a direct child of the second additional object type chosen. The same pattern applies to **View+4** and **View+5**.

Note: This setting is case-sensitive and there must be no spaces between the **View** value and the characters **+1**, **+2**, **+3**, **+4**, or **+5**.

Maximum concurrent export requests

Use the **Concurrent Exports** setting to control the maximum number of Export to Excel (in .xlsx format) requests that are handled at the same time.

Applications > GRCM > Filtered List > Concurrent Exports

Default: 10

Values: In the **Value** field, type a number greater than zero.

Bulk move and rename setting

The Allow Hierarchical Moves setting determines whether users can perform hierarchical move operations. The setting also determines whether users can rename certain object types.

For move operations, the setting determines whether child objects are moved when their parent objects are moved with the  icon in Grid Views.

For rename operations, the setting determines whether a rename operation is allowed for the following object types: business entities, self-contained object types, and object types that are used by the security model.

Applications > GRCM > Object Move > Allow Hierarchical Moves

Default: false

Values:

- true - no restrictions

- **false**

For move operations, child objects are not moved with parent objects for the following object types:

- SOXBusinessEntity
- All objects types that are listed in the **Common > Security > Model** setting (see “[Set the system security model](#)” on page 500)
- All object types that are listed in the **Common > Self Contained Object Types** setting (see “[Configure self-contained object types](#)” on page 501)

For rename operations, the following objects cannot be renamed:

- Business entities (SOXBusinessEntity)
- Object types that are listed in the **Common > Security > Model** setting
- Object types that are listed in the **Common > Self Contained Object Types** setting

If a move or a rename involves a large number of objects, make the change after business hours to reduce the impact on system performance.

Configure HTTP request logging for IBM Watson Language Translator

You can set the level of detail for HTTP request logging for IBM Watson Language Translator by using the **Watson SDK Logging** setting.

When trace logging is enabled for IBM Watson Language Translator, the request URL, HTTP response code, and request headers are included in the trace log by default. You can use the **Watson SDK Logging** setting to change the logging level for the HTTP requests and responses.

The location of the trace log file is `<OP-HOME>/aurora/logs/debug/<server_name>-watson.log`.

This HTTP request logging can help you to troubleshoot network connectivity issues.

Applications > Watson Language Translator > Watson SDK Logging

Default: HEADERS

Values:

- **NONE**: No HTTP logging
- **BASIC**: Minimal logging (request URL and HTTP response code)
- **HEADERS**: Same as Basic, plus the request and response headers
- **BODY**: Same as HEADERS, plus the request and response body



Attention: The BODY logging level has the potential to cause sensitive customer data to be written to the log when resources (such as fields) in a Task View are translated.

Tip: You don't need to restart the application servers when you change this setting.

Custom settings

When enabling new content types and creating your own reports, you may need to create your own custom registry settings. By default, you cannot create or delete settings until you enable the feature.

Common > Configuration > Allow Create and Delete Settings

Default: false

Values:

- **true** - enable the creation and deletion of custom settings.
- **false** - disable the creation and deletion of custom settings.

Creating a custom setting

After enabling **Allow Create and Delete Settings**, you can create custom settings entries in new or existing folders.

Complete the following procedure to create a custom setting:

Procedure

1. Log on as a user with administrative privileges.
2. Click  > **System Configuration** > **Settings**.
3. If you want to create a setting in a folder that doesn't exist, do the following steps:
 - a) Click **New Folder**.
 - b) In **Name**, enter the name of the new folder.
 - c) In the **Folder Path** section, click **Choose**.
 - d) Select the path to the new folder and click **Done**.
 - e) Click **Create**.
- For example, if you want to create the setting **Platform** > **Workflow Implementations** > **OP** > **Expired Process Definition Cache Size**, you need to create the **OP** folder. Enter **OP** as the **Name** and select **/ Platform/Workflow Implementations** as the **Folder Path** to the **OP** folder.
4. Click **New Setting**.
5. In **Name**, enter the name of the new setting.
6. In the **Folder Path** section, click **Choose**.
7. Select the path to the new folder and click **Done**.
8. If you want the value of the setting to be encrypted, select **Encrypted**.
9. Click **Create** to add the new setting to the selected folder.

Deleting a custom setting

After enabling **Allow Create and Delete Settings**, you can delete settings in new or existing folders.

Important: Do not delete any of the predefined settings shipped with IBM OpenPages. These settings are required and cause unexpected behavior in the application if they are removed.

Procedure

1. Log on as a user with administrative privileges.
2. Click  > **System Configuration** > **Settings**.
3. Navigate to the folder that contains the setting to be deleted. Select the desired setting. The **Delete** icon becomes active.
Note: If you select a folder, all settings within that folder are deleted.
4. Click **Delete**.

Copying settings and folders

You can copy individual settings to another location and copy folders to new folders. When you copy a folder, you can give the new folder a name. The settings and subfolders in the folder are copied to the new folder.

Procedure

1. Log on as a user with administrative privileges.

2. Click  > **System Configuration** > **Settings**.
3. Navigate to the folder where the source setting or folder is located.
4. Select the setting or folder that you want to copy.
5. Click **Copy To**.
6. If you are copying a setting, the **Copy Setting To** panel opens. Select the folder in which the new setting will be positioned.
7. If you are coping a folder, the **Copy Folder To** panel opens. Enter the name of the new folder in **Name** and choose a **Target Folder**.
8. Click **Done**. The new setting or folder is created.

Common folder settings

The registry settings in the Common folder are a select list of individual settings.

Maximum rows in exchange rate upload file

Define the **Maximum Import Rows** setting to limit the number of rows that can be in the CSV file that is used to upload currency exchange rates with the  > **System Configuration** > **Currencies** task.

If a CSV file has more rows than defined in the setting, the upload fails and an error message is issued.

Maximum Import Rows

Common > Administration > Currencies > Upload > Maximum Import Rows

Default: 10,000

Values: In the **Value** field, type a number great than zero.

Maximum page size

Define the **Maximum Page Size** setting to limit the number of resources on a page that a UI endpoint can request. Resources can be objects, such as **Business Entities** or **Loss Events**, or strings, such as those on the **Application Text** page, or users on the **Users** page.

Applications > Common > Maximum Page Size

Default: 1000

Values: In the **Value** field, type a number great than zero.

Exclude characters from user names

You can prevent users from creating user names that contain certain characters by using the **Illegal Characters** setting. By default, user names can contain A-Z, a-z, 0-9, and any of the @-! ._/_:/_:*"\#%?<> special characters. You can add any of these characters to the **Illegal Characters** setting to prevent their use.

Common > Security > User Name > Illegal Characters

Default: none

Values: Type the characters that you want to be considered as invalid when creating a user name. For example, if you want the asterisk (*) and ampersand (&) to be considered invalid in user names, enter *& in the **Value** field.

Set the system security model

By default, the security context point at which you can assign role templates to users on objects in the hierarchy is set at the Business Entity (SOXBusEntity) level. You can extend the security context to other objects in the hierarchy to achieve a finer level of control by changing the **Model** setting.

Important:

This is a system-wide setting. Switching the security model after data is loaded (or migrated) into the system is not recommended and requires assistance from IBM OpenPages with Watson Professional Services.

Common > Security > Model

Default:

Values: Type the object type names you want to use as security points.

The syntax for the **Model** setting is: SOXBusEntity/object_type-name

Example: To create a security point for assigning role templates at a Process level, you would enter:

```
SOXBusEntity/SOXProcess
```

Permissions in the Role template could then be assigned at either the Business Entity or Process level, and would include any objects that were created beneath that security context point in the same location.

The maximum number of security context points you can have in the **Model** setting is 3. For example, SOXBusEntity/SOXProcess/RiskAssessment

Disable access control on Role groups

When a role template is disabled, you can use the **Disable Role Group** setting to globally control the security access of users and groups who were previously assigned that role.

Common > Security > Role Templates > Disable Role Group

Default: false

Values:

- true - Users and groups who were previously assigned that role, will lose their access control and application permissions. A disabled role template is removed from the role assignment selection list and cannot be used for further role assignments.
- false - Users and groups who were previously assigned that role, will retain their access control and application permissions.

Related tasks

[“Enabling and disabling a role template” on page 77](#)

Configure self-contained object types

When you define an object type using the **Self Contained Object Types** setting, the behavior of that object type changes for copy, move, and rename operations.

A self-contained object type is an object type that has its own folder and is either part of the role-based security model as defined in the **Model** setting or defined using the **Self Contained Object Types** setting.

For information about the **Model** setting, see [“Role-based security model” on page 67](#).

Note:

- Roles can only be assigned to objects that are defined as security context points through the **Model** setting.
- Defining an object type through the **Self Contained Object Types** setting does not automatically change the folders of existing instances of that type. If instances of the object type you want to define as self-contained already exist, you must contact IBM OpenPages Support for assistance in executing a special PL/SQL script that will go back and create folders for existing instances. This script is maintained

by IBM OpenPages with Watson Customer Services & Support and does not ship as part of the product. Conversely, if an object type is later removed from the self-contained list, no automatic re-foldering occurs. All existing instances retain their dedicated folders.

By default, Business Entities are self-contained objects. For example, if the role-based security model setting is defined as SOXBusEntity/SOXProcess, both Business Entity and Process objects are treated as self-contained objects.

Self-contained object types behave differently than non-self-contained object types for copy, move, and rename operations. The characteristics that distinguish self-contained objects from non-self-contained objects follow.

Self-contained objects:

- Are always created under a parent folder that matches the object name (the same behavior as Business Entities). For example, a process P1 under the North America business entity will have the path /North America/P1/P1.txt
- When copied, all the objects under its hierarchy will also be copied to the target.
- When moved, all the objects under its hierarchy will also be moved to the target.
- Can have only one parent of the same object type.
- Can only be moved to an allowed parent object.
- Cannot be moved to a folder.
- Cannot have their parent folder edited, moved, or renamed.
- Can be renamed by users who have Read+Write access control (ACLs) permission.
- During a copy operation, if a naming conflict exists between the source and the target object, the copy operation will fail and the naming conflict resolution choices made by a user are ignored.

Common > Self Contained Object Types

Default: none.

Values: In the **Value** field, type a comma-separated list of object type names.

For example, if you wanted Process and Risk Assessment object types, you would type:
SOXPProcess , RiskAssessment.

Applications > Common > Administration > System Files > Show GRC Folder Structure

Default: false

Values:

- true - _op_software folder and subfolders are displayed
- false - _op_software folder and subfolders are not displayed

Controls whether the GRC Object folder structure and system files are displayed in the  > **System Configuration** > **System Files** task.

Platform folder settings

The registry settings in the Platform folder are a select list of individual settings.

Enable custom REST service

Use the **Enable Custom REST Service** setting to extend the REST services with custom services that are not included in the existing API services.

For more information, see *Extend GRC API with Custom REST Services* in the *IBM OpenPages with Watson GRC REST API Guide*.

Platform > API > Enable Custom REST Service

Default: false

Values:

- **true** - to enable custom REST services
- **false** - to disable custom REST services

Set the sign of an integer returned by dates function

If **Enable date subtraction fix PH51026** is set to **true**, when a user uses the dates function `[$OPSS-ISS:Due Date$] - [$TODAY$]`, it returns a positive integer if the due date is a future date. If **Enable date subtraction fix PH51026** is set to **false**, the dates function returns a negative integer.

Note: This setting is a hidden setting. To show hidden settings, Click  > **System Configuration > Settings** and set **Applications > Common > Configuration > Show Hidden Settings** to **true**.

Platform > Calculation > Enable date subtraction fix PH51026

Default: For new installations of OpenPages 9.0, the default value is true. For systems upgraded from an earlier version of OpenPages, the default value is false because a change to this functionality could cause existing calculations to return unexpected results.

Values:

- **true** - `[$OPSS-ISS:Due Date$] - [$TODAY$]` returns a positive integer if the due date is a future date
- **false** - `[$OPSS-ISS:Due Date$] - [$TODAY$]` returns a negative integer if the due date is a future date

Set the default pageSize for API queries

Use the **Default PageSize** setting to control the default pageSize for queries through the API (REST API and Java API). The **Default PageSize** is used only when running a query that does not specify a pageSize.

For more information, see the *IBM OpenPages with Watson Developer Guide*.

Platform > API > Query > Default PageSize

Default: 50

A value of 50 means that the query results are returned 50 at a time.

Values:

A value of 0 means that no paging is done. The query returns all results at once.

Set localization options

You can configure settings in the Globalization folder to audit translation label changes and set a default language for IBM OpenPages with Watson.

Auditing

Platform > Globalization > Auditing Enabled

Default: true

Values: Enable auditing of changes that are made to translated object and application label text.

- **true** - auditing enabled.
- **false** - auditing disabled.

This option must be set to true to allow new application strings to load.

Default locale

Platform > Globalization > Default Locale

Default: en_US

Values: Set the language to use to display the application user interface by default.

Note: You can override the default locale setting. Click  > **Change Locale** to see a list of product languages. This language setting controls the language of the product except for the login page. Select a locale and click **Save**.

The following list identifies the supported locale code values with their corresponding language:

- de_DE (German)
- en_GB (U.K. English)
- en_US (U.S. English)
- es_ES (Spanish)
- fr_FR (French)
- it_IT (Italian)
- ja_JP (Japanese)
- pt_BR (Brazilian Portuguese)
- zh_CN (Simplified Chinese)
- zh_TW (Traditional Chinese)

For example, to set the default language of the application interface to German, type de_DE in the **Value** field.

Configure primary associations

When a child object has multiple parent objects, the **Association Heuristic** setting controls how the system reassigned a new primary parent after the child object has been created.

A new primary parent is assigned to a child object whenever the child object becomes disassociated from its primary parent. You can change how primary parent objects are reassigned to disassociated child objects.

Platform > Repository > Resource > Association Heuristic

Default: **Chronological**

Values: Type one of the following values:

- **Chronological** - the reassignment of a primary parent is based on the earliest creation date and time of an association.
- **Folder Context** - the reassignment of a primary parent is based on the folder path within the context of the business entity.

For example, control C1 has multiple risk parents: R1, R2, R3, and R4 (primary parent) and the object associations were created in the following chronological order:

Table 157. Parent folder path and associated child folder path

Parent folder path	C1 Child folder path
/BE1/SBE2/R2	/BE1/SBE1/C1
/BE1/SBE1/R1	/BE1/SBE1/C1
/BE1/SBE3/R3	/BE1/SBE1/C1
/BE1/SBE4/R4 (primary parent)	/BE1/SBE1/C1

If you disassociate the primary parent, R4, from C1, although R2 is chronologically the earliest association to C1, R1 is reassigned as the primary parent. This is because R1 and C1's folder paths match (/BE1/SBE1).

Note: If no folder path matches the child object, the chronological order is used.

Configure the host setting

If you have older JSP reports and want to send email notifications to users from these older JSP-based reports or the Notification Manager utility, configure the host setting.

Note: This setting is only used for backward compatibility.

Platform > Publishing > Mail

Default: none

Values: Click the name of a setting that is listed in the following table and change the value as follows:

Table 158. Host settings

Setting	Description
Enabled	Set the value to true.
From Address	Verify or enter the email address of the sender using a valid email address and format. By default, the value is: sysadmin@yourcompany.com
Host	Verify or enter the name of your mail server. By default, the value is: mail.yourcompany.com

Configure the Cognos URL settings

The URLs for IBM Cognos Analytics are stored in settings. Update these settings when the IBM Cognos Analytics host or port numbers change.

Platform > Reporting

Table 159. Settings that contain port numbers for IBM Cognos Analytics

Setting	Description
Platform > Reporting > Cognos Dispatcher Service URL	Specifies the URL of the IBM Cognos Analytics dispatcher service. See Gateway URI in Cognos Configuration. For example: <code>http://<server_name>:<port>/ibmcognos/bi/v1/Disp</code>
Platform > Reporting > Cognos SDK URL	Specifies the URL of the IBM Cognos Analytics biapp service. See External Dispatcher URI in Cognos Configuration. For example: <code>http://<server_name>:<port>/p2pd/servlet/dispatch</code>

Table 159. Settings that contain port numbers for IBM Cognos Analytics (continued)

Setting	Description
Platform > Reporting > Cognos Logout URL	<p>Specifies the IBM Cognos Analytics logout URL.</p> <p>For example:</p> <pre>http://<server_name>:<port>/ibmcognos/ bi/v1/disp?b_action=xts.run&m=portal/ logoff.xts&h_CAM_action=logoff</pre>

Cross-context sharing

You can use the **Cross context sharing** setting to affect whether any non-primary links to objects outside the context (scope) of a copy operation are included or ignored during a copy operation.

When cross-context sharing is enabled, copy operations maintain non-primary links to objects outside the context of the copy. When it is disabled, non-primary links to objects outside the context of the copy are ignored.

For example, in the following example hierarchy , Control C1 was originally created under Risk R1, and R1 has a primary association to C1. Risks R2 and R3 have non-primary associations to C1. If a user copies Process P2 from BE2 to BE3, the link to C1 is maintained if the **Cross context sharing** setting is enabled (set to true). If the setting is disabled (set to false), the copied tree ends at R3 as the non-primary association to C1 is outside the context of the copy operation. If the user copies P1 from BE1 to BE3, the current state of the **Cross context sharing** setting is irrelevant. The non-primary association from R2 to C1 falls within the context of the copy operation.

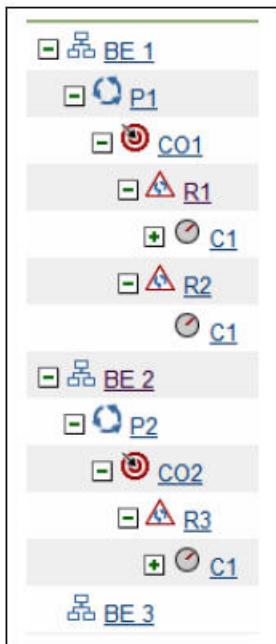


Figure 65. Sample Hierarchy

Platform > Repository > Resource > Copy > Cross context sharing

Default: false

Values: In the **Value** field, type one of the following values:

- **true** - Cross-context sharing is enabled and the copy operation maintains any non-primary links to objects that are outside the scope (context) of the copy.

- **false** - Cross-context sharing is disabled and the copy operation ignores any non-primary links to objects that are outside the scope (context) of the copy.

Platform Reporting Framework folder settings

The settings in the **Platform > Reporting Framework V6** folder apply to the reporting framework, which is used with IBM Cognos Analytics.

Note: "V6" refers to the latest framework version, not to any specific OpenPages release number.

For more information, see the following topics:

- [Chapter 29, “Configuring and generating the reporting framework,” on page 799](#)
- [“Configuring settings that apply to all framework models” on page 806](#)
- [“Configuring framework models ” on page 810](#)

Reporting Schema folder settings

The **Platform > Reporting Schema** folder settings represent a selected list of individual settings.

Add indexes for fields in the reporting schema

You can add an index to any RT_ table in the database through the **Create Index on Fields** setting.

Before configuring this setting, complete the following tasks:

- Review this task with your database administrator and IBM OpenPages Support.
- Test the change by manually creating the index in the database before making a permanent change in IBM OpenPages with Watson.

You can create a string up to 4000 characters.

Configure this setting only after careful analysis of your data query patterns. Adding too many indexes to a table can harm performance.

After modifying this registry entry, you can implement your index changes by either re-creating or updating the reporting schema.

Platform > Reporting Schema > Create Index on Fields

Default: none.

Values: In the **Value** field, enter an index in the following format:

```
ObjectTypeName1= [FieldGroupName1.PropertyName1,...,
FieldGroupNameN.PropertyNameN]
|ObjectName= [FieldGroupName1.PropertyName1
,...,FieldGroupNameN.PropertyNameN]
```

Where:

ObjectTypeName1 is the name of the object type you want to add an index to.

FieldGroupName1 is a bundle definition associated with the object.

PropertyName1 is the name of a property in the bundle.

Note:

- Vertical bars (|) separate multiple index strings.
- Commas (,) separates columns inside an index.

For more information about re-creating or updating the reporting schema, see [“Changes that require the reporting schema to be updated or re-created” on page 117](#).

Example 1: Adding an index on name and reporting period

You want to add an index on the Risk object type that includes the name and reporting period. The string would look as follows:

```
SOXRisk = [Core Attributes.Resource Name,  
          Reporting Period Attributes.Reporting Period ID]
```

The Core Attributes bundle includes all of the following system parameters:

- Latest Resource Version
- Resource Check Out Status
- Resource Check-in Date
- Resource Checked in By
- Resource Checked Out By
- Resource Content Type
- Resource Creation Date
- Resource Creator
- Resource Description
- Resource File Type
- Resource Full Path
- Resource ID
- Resource Name
- Resource Parent Folder
- Resource Subresource Type
- Resource Type
- Resource Visibility

The Reporting Period Attributes bundle includes the following reporting period parameters:

- Reporting Period ID
- Reporting Period Name

Example 2: Adding an index on a custom field

You created a custom field called Test Reviewer on the Test object type and now want to add an index to this custom field. The index for the Test Reviewer custom field would be as follows:

```
S0XTest = [OpenPagesStandardTest.Test Reviewer]
```

Example 3: Adding an index for quick filters and custom simple strings

Indexes can help the performance of certain searches with Quick Filters and filters on custom simple string fields (except users and user groups).

The usual indexing technique is not applicable here, because Quick Filters and filters on custom simple string fields are commonly case insensitive and commonly implement "contains" logic. As such, even if a database index existed on the filtered field, it would not be used.

A typical use case is as follows:

- Filter performance appears inadequate.
- The user executing a filter has IBM OpenPages security access to a small fraction of the data.
- The number of records is high. This is a function of the number of object instances in the current reporting period and the number of reporting periods in the system.
- The width of records is high. This is a function of the number of custom properties.

For example, loss event data may be tightly restricted within a company. As such, indexing the LossEvent object type could improve filter performance.

```
LossEvent = [Reporting Period Attributes.Reporting Period ID,  
Core Attributes.Resource Parent Folder]
```

It is beneficial to filter on security access before applying any property filter. The security access filter will filter out a large percentage of data, leaving the property filter to work on fewer records.

Such an index will benefit all the filters on a given Object Type, so it only needs to be created once per Object Type.

Re-create indexes for a reporting schema when it is updated

You can enable or disable the re-creation of custom indexes for a reporting schema when it is updated by using the **Recreate Custom Indexes On Update** setting.

By default, custom indexes are re-created on update.

Platform > Reporting Schema > Recreate Custom Indexes On Update

Default: true.

Values: **true, false**

For more information about updating the reporting schema, see [“Updating the reporting schema” on page 121](#).

Security settings

The **Platform > Security** settings represent an individual settings to configure settings.

All of the following actions are accessed from the **Platform > Security** folder.

Configure anti-virus scanning for imported files

You can use Clam AntiVirus (ClamAV) to scan files for viruses and malware before the files are imported into OpenPages. Files that fail the scan are not uploaded.

ClamAV is an open source, cross-platform, anti-virus toolkit. ClamAV is the only anti-virus software that is supported by OpenPages for the scanning of files.

ClamAV has the following features:

- It is available for Linux, Windows, Mac OS X, and Docker.
- The ClamAV virus database is frequently updated.
- It supports many file formats.

For more information about ClamAV, see the ClamAV documentation at <https://docs.clamav.net/>.

Before you begin

A ClamAV server is not provided with an OpenPages installation. You must install ClamAV on a server that OpenPages can access.

About this task

To ensure that files are scanned before they are uploaded, you must specify the ClamAV server and port and you must enable anti-virus scanning.

File uploads are not affected when anti-virus scanning is disabled.

You can configure OpenPages to perform the following tasks:

- Block all uploads if the anti-virus server is unreachable.
- Time out when an anti-virus scan request to the remote server has not been answered after a set number of milliseconds.
- Only scan files up to a set maximum size.
- Perform a set number of retry attempts when a file is being scanned.

Procedure

1. Click  > **System Configuration** > **Settings**.
2. Set **Platform** > **Security** > **Antivirus Scan** > **Enabled** to **true**.
3. Set **Platform** > **Security** > **Antivirus Scan** > **ClamAV Server** to the hostname or IP address where the ClamAV server is located.
The default value is **http://localhost**.
4. Set **Platform** > **Security** > **Antivirus Scan** > **ClamAV Port** to the port number of the ClamAV server.
The default value is **3310**.
5. Optional: To block all files from being uploaded if the ClamAV server is unavailable, set **Platform** > **Security** > **Antivirus Scan** > **Block Uploads if Unreachable** to **true**.
The default value is **false**.
6. Optional: To specify a timeout for anti-virus scan requests to the remote server, set **Platform** > **Security** > **Antivirus Scan** > **ClamAV Timeout** to a value in milliseconds. A value of **0** means the request will not time out.
The default value is **5000**.
You might need to increase this value if you are importing complex files, such as compressed files, that are bigger than 100 MB.
7. Optional: To specify a maximum size of file for scanning, set **Platform** > **Security** > **Antivirus Scan** > **Maximum File Size** to a size in MiB. A value of **0** means there is no maximum.
When you set this value to be greater than 0, larger files are skipped.
The default value is **0**.
8. Optional: To specify the number of retry attempts to make when scanning a file, set **Platform** > **Security** > **Antivirus Scan** > **Retry Attempts** to an integer value.
The default value is **3**.
You might need to increase the number of retry attempts if you are importing complex files, such as compressed files, that are bigger than 100 MB.

Redirect the security logoff link

By default, click **Log Off** in the header pane to log the user out of IBM OpenPages with Watson.

If you are using single sign-on (SSO), you can change the page that is displayed after you log off by modifying the value of **Logout URL**.

Note: If you are not using single sign-on, you cannot redirect the logout link.

Platform > **Security** > **Logout URL**

Default: none

Values: In the **Value** field, type a qualified URL.

Configure security for user logon

Configure settings to prevent users from logging in to IBM OpenPages with Watson.

Locking a user account prevents the user from logging in to OpenPages with Watson. However, the user is still an active user in the system, and can be selected through the user selector.

Users can be locked automatically if they exceed a set number of unsuccessful login attempts. If the user is locked out because they forgot their password, you can unlock their account and reset their password. For more information, see “[Modifying user accounts](#)” on page 49. If there is concern that the login attempts are malicious, contact your security department.

The **User Locking** folder contains the following settings that control the locking behavior of OpenPages with Watson.

Platform > Security > User Locking

Values: Click a setting and type a value in the **Value** field.

Table 160. Locking values

Value	Description
Enabled	Sets whether the User Locking settings are active. When the value is set to <code>true</code> , users are locked after they unsuccessfully try to log in more than the Maximum Allowed Attempts. If <code>false</code> , there is no limit to failed login attempts and the remaining settings are not honored.
Maximum Allowed Attempts	Sets the maximum number of times that a user can unsuccessfully try to log in to the application before the account is locked. The Unsuccessful Login Window setting applies a time window on the attempts.
Timeout	Sets the amount of time (in minutes) that the user account is locked after failing to log in. After the timeout is over, the user can attempt to log in again.
Unsuccessful Login Window	Sets a time window (in minutes) for the log in attempts. The system checks the number of failed attempts within the time window. For example, if the Maximum Allowed Attempts is 3, the Timeout is 60, and the Unsuccessful Login Window is 10: <ul style="list-style-type: none">• If a user makes two unsuccessful login attempts and then waits 10 minutes, the account is not locked and the time window and number of attempts are reset to zero. The user can again make three attempts to log in.• If a user makes three unsuccessful login attempts within 10 minutes, the account is locked. The user must wait 60 minutes and can again make three attempts to log in.

Security cross-site scripting filter settings

Cross-site scripting (XSS) is a computer security vulnerability that allows malicious attackers to inject client-side script into web pages viewed by other users. You can use the **Cross-site Scripting Filter** setting to check all HTTP GET requests sent to IBM OpenPages with Watson. The **Cross-site Scripting Filter** setting enables basic filtering of common attacks. The **Advanced XSS Filter** setting turns on more aggressive filtering of JavaScript actions.

For more information about the **X-XSS-Protection** header setting, see [“Configure the HTTP response headers” on page 513](#).

To allow certain HTML elements or attributes to pass through this filter, see [“Configure the security safe tags setting” on page 512](#).



Attention: The XSS filter blocks attempts to save text fields that contain JavaScript. The XSS filter also blocks updates to items that were created and saved with JavaScript when the XSS filter was disabled. Text fields that contain JavaScript are not supported.

Note: These settings are hidden by default. To display them, see [“Show hidden settings” on page 479](#).

Platform > Security > Cross-site Scripting Filter

Default: true

Values: In the **Value** field, type one of the following values:

- true - Cross-site filtering is enabled.
- false - Cross-site filtering is disabled.

Restart all application servers in your cluster to enable the change. For information, see [Chapter 25, “Starting and stopping servers,” on page 709](#).

Platform > Security > Advanced XSS Filter

Default: true

Values: In the **Value** field, type one of the following values:

- true - Advanced XSS filtering is enabled.
- false - Advanced XSS filtering is disabled.

Restart all application servers in your cluster to enable the change. For information, see [Chapter 25, “Starting and stopping servers,” on page 709](#).

Configure the security safe tags setting

When the **Cross-site Scripting Filter** setting is enabled, certain HTML elements are blocked by that filter.

For more information on enabling this filter, see [“Security cross-site scripting filter settings” on page 511](#). You can use the **Safe Tags** setting to globally allow certain HTML elements to pass through the filter.

For example, your company uses embedded forms to capture information that is provided by users. The embedded form contains the HTML `form` element, which is passed in an HTTP request. By default, the **Cross-site Scripting Filter** setting is enabled so the `form` element is blocked. To allow user input in an embedded form to be passed in an HTTP request, you would add the HTML `form` element to the **Safe Tags** value list as follows:

```
style, form
```

Tip: In the user interface, the **Safe Tags** setting is not displayed. You can add it manually in the XML file. Use the following path: /OpenPages/Platform/Security/Safe Tags

Safe Tags

Default: By default, the HTML `style` element is the only element that is allowed through the XSS filter.

Values: In the Value parameter, type the name of an HTML element or attribute. Multiple values must be separated by a comma.

Restart all application servers in your cluster to effect the change. For details, see [Chapter 25, “Starting and stopping servers,” on page 709](#).

Configure the HTTP response headers

Platform > Security > Headers

Configure the HTTP response header settings to add security that controls what a browser renders on a page. There are four settings:

- **Content-Security-Policy**

Controls from where the page can download source. If enabled, the value of this setting is merged with the value set by the system and added as a header to all page responses. The X-Content-Security-Policy header will also be set. The system value also includes the hostname of the reporting server and some other settings required by the application.

The setting uses the Content Security Policy tool syntax. For more information, see [Content Security Policy](#).

Example value: default-src myserver.com:100

- **X-Frame-Options**

Controls where a page can get source to render in a frame. This header is added to all page responses. The value here overrides the default, which is SAMEORIGIN.

Example value: DENY

- **X-Content-Type-Options**

Prevents the browser from trying to determine the content-type of a resource that is different than the declared content-type. This header is added to all page responses. To override the default, enter an invalid string, for example, a space character.

Default: nosniff

- **X-XSS-Protection**

Enables X-XSS-Protection header on server responses. If X-XSS-Protection is set to true, the X-XSS-Protection header is set to 1; mode=block. For more information, see [“Security cross-site scripting filter settings” on page 511](#).

Default: false

Configure allowed character combinations for URLs

You can use the **Allowed Suspicious Character Combinations** setting to enable certain character combinations in URLs.

By default, IBM OpenPages with Watson blocks URLs that contain unexpected or suspicious character combinations. If you attempt to go to a URL in OpenPages that contains unexpected characters, you are logged out of the application. See the `aurora.log` file on the application server for details about the character combination that was detected in the URL.

If OpenPages blocks URLs due to unexpected character combinations and the URLs are valid for your deployment, modify this setting to allow the character combination in URLs.

Note: Use a loader file to update this setting. Do not modify it in the user interface.

Platform > Security > Allowed Suspicious Character Combinations

Default: None

Values: Use a loader file to update the **Value** field.

Each character combination must be separated by a new line. Use `\xA`; to create a new line.

If one of the characters that you want to allow is a special character, such as " (quotation mark), you must escape it, ".

For example, suppose you want to allow ' ; (a single quotation mark followed by a semicolon) and " , (a double quotation mark followed by a comma). In this case, use a loader file like this sample file:

```
<openpagesConfiguration xmlFormatVersion="1.27">
<registry>
<registryEntry name="/OpenPages/Platform/Security/Allowed Suspicious Character
Combinations"
description="Certain character combinations are considered suspicious by the XSS filter. If
you see such a message in the aurora.log and the character combination is actually valid,
you can use this setting to allow it. Note that this setting may not be changed in the UI.
You must use a loader file."
hidden="false"
encrypted="false"
protected="true"
value="';&#xA;&quot;, />
</registry>
</openpagesConfiguration>
```

Configure audit event settings

The audit event setting determines whether management events are audited.

Platform > Security > Audit Management Events

Default: false

Values: In the **Value** field, type one of the following values:

- true - Events related to users are audited. Examples of such events are: adding and modifying users and user groups, promoting and demoting a user to a superuser, enabling and disabling users, and adding and removing users from group memberships.
- false - Events related to users are not audited.

Enable users to get error message details for troubleshooting

Enabling this setting allows users to get error message details that include a stack trace for troubleshooting problems.

Note: Before you enable this setting, ensure that the users have the Enhanced Error Messaging application permission. For more information about setting application permissions, see “[Defining application permissions](#)” on page 51. For more information about the Enhanced Error Messaging application permission, see “[Application permissions not contained under the SOX heading](#)” on page 58.

If the **Enhanced Error Messaging** setting is set to **true**, a **Show details** button is displayed in error message boxes.

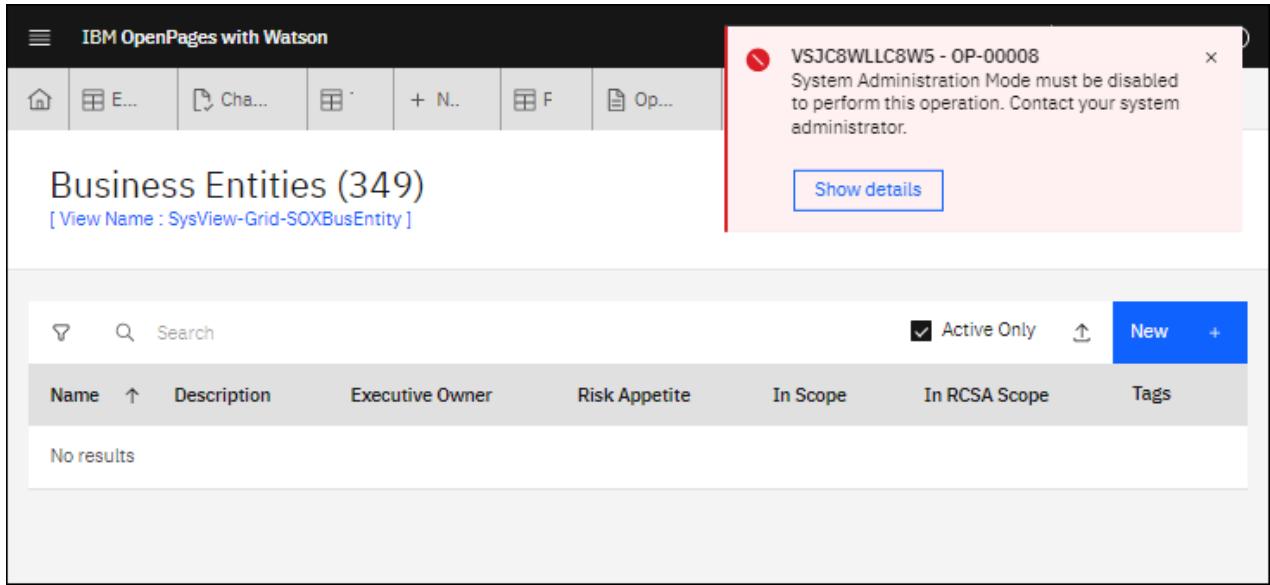


Figure 66. An error message box with the **Show details** button

When a user clicks **Show details**, the **Notifications** page is displayed with more information about the error.

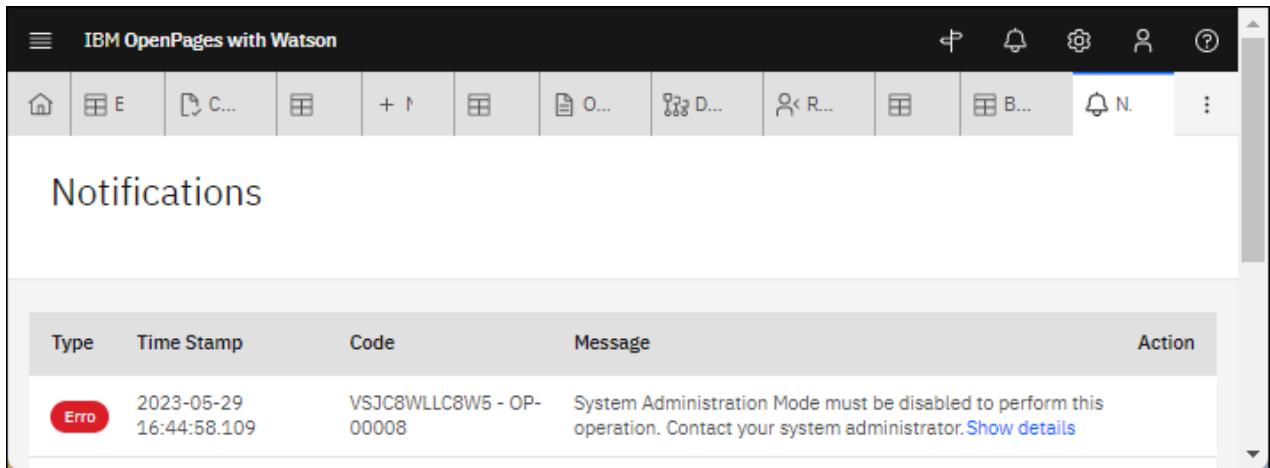


Figure 67. Notifications page showing the error message details

Note: For security reasons, only enable this setting when a user is troubleshooting a specific issue and disable it when the troubleshooting is complete.

Platform > Security > Enhanced Error Messaging

Default: false

Values: In the **Value** field, type one of the following values:

- true - Allows users who have the Enhanced Error Messaging application permission to click a **Show details** button that is displayed with error messages. The error message details include a stack trace.
- false - Error messages do not display a **Show details** link.

User Preferences folder settings

The User Preferences folder settings represent a selected list of individual settings in the User Preferences folder.

All of the following actions are accessed from the Platform folder.

Set alert notification behavior

Set which alert notifications are displayed to application users in the Alerts folder. You can select various alert notification settings in the **Alerts** page.

User Preferences > Alerts

Default: false.

Values: Select the name of a setting on the **Alerts** pane. In the **Value** box, type one of the following values:

- **true** - An alert is displayed to application users.
- **false** - No alert is displayed to application users.

For example, you configured dependent fields or dependent picklists for an object type and you want to alert users that different values for particular fields are available depending on their selection.

Under the Alerts folder, you can set the values in the **Picklist Options Changed** and **Picklist Values Removed** settings to **true** so each time a user changes a value in one of these fields, an alert notifying the user that values have changed is displayed.

Chapter 21. Configuring the global search feature

To optimize the performance of IBM OpenPages with Watson global search, you can enable or disable what can be searched, tune the search settings, and change other properties in the properties file.

About this task

For more information about using global search, see the topic *Searching for objects* in the *IBM OpenPages with Watson User Guide*.

Note: This feature is not applicable in IBM OpenPages for IBM Cloud Pak for Data.



Attention:

- Security rules and evaluating security rules adds a level of overhead to user operations, including global search. The more complex the rule, the more time it takes to evaluate the rule. The number of rules that are being implemented also affects performance.

In the case of global search, a security rule that extends read access can increase search time for users who do not have sufficient read access for an object type. Similarly, a security rule that restricts read access can increase search time for users who do have access to that object type through role-based security.

- Global search must be disabled before running the OPBackup and OPRestore utilities.

For information about configuring global search to use Secure Sockets Layer (SSL), see the following topics:

- [“Setting up a secure connection for the global search service” on page 673](#)
- [“Enabling a secure connection between the search server and the database server” on page 676](#)
- [“Disabling the TLS database connection between the search server and the database server” on page 677](#)

Setting up global search

Before you use IBM OpenPages with Watson global search in production (or even in a test environment against a large set of data), it is recommended that you first set up global search for a small set of data, such as a few thousand records in a test environment, and using the default settings.

Before you begin

Learn more about global search by reading the commonly asked questions listed in [“Global search FAQs” on page 542](#).

About this task

You can set up search on the same server as the one hosting the IBM OpenPages with Watson application. Make sure that the server has at least 12 GB of RAM to host both the IBM OpenPages with Watson application and search feature.

Procedure

1. Install IBM OpenPages with Watson using the default settings. Make sure that you also install the Search Server component. Specify the default values for all the fields. For more information, see the topic *Search server post installation tasks* in the *IBM OpenPages with Watson Installation and Deployment Guide*.

2. Follow the steps in the topic *Copying database driver files to the search server* in the *IBM OpenPages with Watson Installation and Deployment Guide* to copy the JDBC database driver and start the search server.
3. Log in to IBM OpenPages with Watson as a user with administrative privileges.
4. Click  > **System Configuration** > **Global Search** and click **Create**.
Create appears only on initial enablement.
Creating the index also enables global search.

What to do next

For more information about configuring UI components that provide users access to global search, see [“Adding a Search panel” on page 232](#).

For more information about using global search, see the topic *Searching for objects* in the *IBM OpenPages with Watson User Guide*.

For more information about administering global search, see [“Customizing global search” on page 523](#)

Setting login information for the search server

You can set the user names and passwords that the search server uses to access the database server and the IBM OpenPages with Watson global search service (Apache Solr). You can set the login information before you enable global search.

About this task

When you set up passwords, they are encrypted automatically to ensure secure and authenticated access.

If you have enabled global search and you want to change the login information, see [“Changing the database connection information for the search server” on page 525](#).

Procedure

1. On the search server, open a command prompt.
2. To change the login information that the search server uses to login to the database, enter the following commands:

On Microsoft Windows operating systems,

```
cd <SEARCH_HOME>/OPSearch/opsearchtools/
opsearchtool.cmd setdbuserpassword -username current-username -password "current-password"
-newusername new-username -newpassword "new-password"
```

On Linux operating systems,

```
cd <SEARCH_HOME>/OPSearch/opsearchtools/
./opsearchtool.sh setdbuserpassword -username current-username -password 'current-password'
-newusername new-username -newpassword 'new-password'
```

Table 161. Parameters to change the database login information

Parameter	Description
<i>current-username</i>	The database username The value is the username that you entered in the OpenPages installation app when you configured the search server.

Table 161. Parameters to change the database login information (continued)

Parameter	Description
<i>current-password</i>	The password of the database user The value is the password that you entered in the OpenPages installation app when you configured the search server.
<i>new-username</i>	The new database username
<i>new-password</i>	The new password for the database user

For example, the following command changes the password to dbNEWpassword, but keeps the same database username:

```
opsearchtool.cmd setdbuserpassword -username dbuser -password "dbpassword"
-newusername dbuser -newpassword "dbNEWpassword"
```

The following command changes both the database username and the password:

```
opsearchtool.cmd setdbuserpassword -username dbuser -password "dbpassword"
-newusername dbNEWuser -newpassword "dbNEWpassword"
```

3. To change the login information for the global search service (Apache Solr), enter the following commands:

On Microsoft Windows operating systems,

```
cd <SEARCH_HOME>/OPSearch/opsearchtools/
opsearchtool.cmd setsolruserpassword -newusername new-solr-username -newpassword new-solr-
password
```

On Linux operating systems,

```
cd <SEARCH_HOME>/OPSearch/opsearchtools/
./opsearchtool.sh setsolruserpassword -newusername new-solr-username -newpassword new-solr-
password
```

Table 162. Parameters to change the global search service login information

Parameter	Description
<i>new-solr-username</i>	The new username for the Solr service The Solr user does not need to be an OpenPages user.
<i>new-solr-password</i>	The new password for the Solr user

Note: You do not need to provide the current username and password to change and encrypt the password for the global search service. The script uses the current login information of the database server for authentication before it allows the change. The default username and password is OpenPagesAdministrator / OpenPagesAdministrator.

For example, the following command sets the username to solruser and the password to solrpassword:

```
opsearchtool.cmd setsolruserpassword -username solruser -password solrpassword
```

4. Start the global search services.

For more information, see “[Starting the global search services by using a script](#)” on page 712.

5. If required, set up SSL for the Solr service.

For more information, see “[Setting up a secure connection for the global search service](#)” on page 673

What to do next

When you update the user name and password, the changes are applied only to the search server. You must update the database server as well to ensure the login information is synchronized.

Changing the login information for the search server

You can change the user names and passwords that the search server uses to access the database server and the global search service (Apache Solr).

About this task

When you change the passwords, they are encrypted automatically to ensure secure and authenticated access.

Procedure

1. Log on to OpenPages as a user with administrative privileges.
2. Click  > **System Configuration** > **Global Search**.
3. Click **Disable** to disable the global search component.
4. Stop the global search service.

For more information, see “[Stopping the global search services by using a script](#)” on page 713 or “[Stopping the global search services](#)” on page 715.

5. Change the database user name or password.

For more information, see “[Changing password references](#)” in the *IBM OpenPages with Watson Administrator’s Guide*.

6. Change the login information to use for the database server and Apache Solr.

For more information, see “[Setting login information for the search server](#)” on page 518.

7. Start the global search services.

For more information, see one of the following topics:

- “[Starting the global search services by using a script](#)” on page 712
- “[Starting the global search services on Windows](#)” on page 713
- “[Starting the global search services on Linux](#)” on page 714

8. Click  > **System Configuration** > **Global Search**.

9. Click **Enable** to enable the global search component.

10. If required, set up SSL for the global search service.

For more information, see “[Setting up a secure connection for the global search service](#)” on page 673 in the *IBM OpenPages with Watson Installation and Deployment Guide*.

What to do next

When you update the user name and password, the changes are applied only to the search server. You must update the database server as well to ensure the login information is synchronized.

Using OPBackup and OPRestore when global search is enabled

Before you run OPBackup or OPRestore, global search must be disabled.

About this task

OPBackup is the IBM OpenPages with Watson backup utility that backs up the necessary product files and database content on the server where it is run. The OPBackup utility creates a backup file that can be used by the OpenPages restore utility (OPRestore).

Procedure

1. Disable global search:
 - a) Log in as an administrator.
 - b) Click **Administration > Global Search > Disable**.
2. Perform OPBackup or OPRestore. For more information, see “[The OPBackup utility \(Db2\)](#)” on page [548](#) or “[The OPBackup utility \(Oracle\)](#)” on page [581](#).
3. Enable global search:
 - a) Log in as an administrator.
 - b) Click **Administration > Global Search > Enable**.
4. To re-create the global search index:
 - a) Log in as an administrator.
 - b) Click **Administration > Global Search > Disable**.
 - c) Click **Administration > Global Search > Drop**.
 - d) Click **Administration > Global Search > Create**.



Attention: If you run the OPRestore utility, the search index becomes out of sync with the restored data in the OpenPages database. As a result, global search results might be inaccurate and incomplete. To prevent this, you must re-create the global search index. You can re-create the global search index before or after the database restore operation.

Enabling and disabling global search

You can enable or disable global search.

About this task

For example, if your organization stipulates that you update passwords periodically, you can disable the global search component, reset user names and encrypt passwords, then enable the global search component.

If you need to troubleshoot a problem with enabling and disabling global search, or if you prefer using a CLI, you can still use the command line to enable and disable global search. For more information, see [How to automate Solr tasks?](#).

Procedure

1. Log on to OpenPages with Watson as a user with administrative privileges.
2. Click  > **System Configuration > Global Search** and click **Disable**.
3. Click  > **System Configuration > Global Search** and click **Enable**.

Recreating the index for global search

You can re-create the index for global search.

About this task

Important: If you have upgraded or migrated to IBM OpenPages with Watson 9.0.0 from 8.2.0.x, you must re-create the index for global search. If you do not re-create the index, global search will not function.

If you need to troubleshoot a problem with re-creating the index for global search, or if you prefer using a CLI, you can still use the command line to re-create the index. For more information, see [How to automate Solr tasks?](#)

Procedure

1. Log on to OpenPages with Watson as a user with administrative privileges.
2. Click  > **System Configuration** > **Global Search** and click **Disable**.
3. Click **Drop** to drop the search index.
Wait for the drop process to complete.
4. Click **Create** to re-create the search index.

Enabling and disabling file attachment searching

From the global search administration page, you can toggle between enabling and disabling the file attachment search component for all search-enabled file types.

Before you begin

You must make sure that the openpages-storage location is accessible to the global search server before enabling file attachment search. For more information, see “[Setting the root path location for file attachment search](#)” on page 541.

About this task

In a fresh installation, file attachment search is enabled by default. In an upgrade installation, file attachment global search is disabled.

Procedure

1. Log on to OpenPages with Watson as a user with administrative privileges.
2. Click  > **System Configuration** > **Global Search**.
3. Click **Disable File Search** to disable the file search component.
4. Click **Enable File Search** to enable the file search component again.
5. Click **Check for Updates**.
6. When the check for updates is completed, click **Update** for the changes to take effect.

Enabling attachment file types for global search

From the File (SOXDocument) object type definition, you can specify which file types are enabled or disabled for file attachment global search.

Before you begin

Log on to OpenPages with Watson as a user with administrative privileges.

Procedure

1. Enable overall global search for file attachments. For more information, see “[Enabling and disabling file attachment searching](#)” on page 522.
2. Enable global search for specific file types on the File (SOXDocument) object type. For more information, see “[Enabling and disabling global search for file types](#)” on page 204.
3. Click  > **System Configuration** > **Global Search** and click **Check for Updates**.
4. When the check for updates is completed, click **Update** for the changes to take effect.

Customizing global search

You can customize and configure global search to meet your organizational needs and policies.

Before you enable global search, you might want to evaluate your IBM OpenPages with Watson database schema and based on your organizational policy, determine which object types and their fields should be enabled for global search. As your IBM OpenPages with Watson database schema evolves, such as when you add or remove object types or fields, you can update global search to reflect those changes.

For information about configuring global search the first time you use it, see “[Example: customizing global search on initial enablement](#)” on page 524. For information about configuring global search after initial enablement, see “[Example: adding or removing object types and fields with an already-enabled global search](#)” on page 525.

Enabling or disabling object types or fields for global search

Most object types and fields that are already enabled for global search. You can change which object types and fields are enabled for global search before or global search is enabled.

About this task

For an example, see “[Example: customizing global search on initial enablement](#)” on page 524.

Setting **Global Search** to **True** or **False** does not take effect until you use the **Check for Updates** command, followed by the **Update** command.

- After you add an object type or field to the reporting schema, you must decide whether the object type or field is enabled for global search. After you set **Global Search** to **True** or **False**, you must use the **Check for Updates** command, followed by the **Update** command.
- If you exclude a field from the reporting schema, disable global search for the field.
- After you enable or disable file attachment search, or after you add or remove MIME types from file attachment search, you must use the **Check for Updates** command, followed by the **Update** command. For more information, see “[Enabling and disabling file attachment searching](#)” on page 522 and “[Enabling attachment file types for global search](#)” on page 522.
- If you enable encryption on a field that is enabled for global search, you must disable global search before you can enable it for encryption. For more information, see “[Enabling and disabling global search](#)” on page 521. After you enable encryption, you must use the **Check for Updates** command, followed by the **Update** command.
- If you import object types and fields by using FastMap, and the imported data either has new object types or fields, or makes changes to existing object types or fields to the global search setting, you must use the **Check for Updates** command, followed by the **Update** command.
- If you import object types and fields by using Environment Manager or Object Manager, and the imported data has new object types or fields, or makes changes to existing object types or fields to the global search setting, you must use the **Check for Updates** command, followed by the **Update** command.
- If you delete an object type or a field, you must use the **Check for Updates** command, followed by the **Update** command.

Note: Anytime you click **Update**, some sort of reindexing takes place. However, when you click **Check for Updates**, no indexing occurs.

For example:

- When you add or remove fields from an object type, or add or remove MIME type from file search, this results in reindexing affected object types. The time this takes depends on how many records are under the affected object type.
- When you add a new object type, this results in reindexing the newly added object type. The time this takes depends on how many records are under the affected object type.
- Removing an object type does not result in reindexing that object type, other than the object type is removed from the index. This occurs immediately.

Procedure

1. Log in to IBM OpenPages with Watson with administrative privileges.
2. Click  > **Solution Configuration** > **Object Types**.
3. Select the object type or field for which you want to enable or disable global search.
4. Click **Edit**.
5. Set **Global Search** to **True** or **False**.
6. Click **Done**.
7. Click  > **System Configuration** > **Global Search** and click **Check for Updates**.
8. When the process completes, check the logs for changes such as added or removed object types and fields. You can go back and make more changes and click **Check for Updates** to see a log of updated changes.
9. When you are satisfied with your changes, click **Update** to force the changes onto the global search index.

Example: customizing global search on initial enablement

You can customize global search to meet your requirements when you first enable it.

About this task

This example assumes that you have not yet enabled global search. You decide to eliminate the object type **SOXSubaccount** and the field **Owner** of the object type **SOXRisk** from being searchable in global search.

Procedure

1. Log in to IBM OpenPages with Watson with administrative privileges.
2. Click  > **Solution Configuration** > **Object Types**.
3. Select the object type labeled **Sub-Account** with the name **SOXSubaccount**.
4. Click **Edit** and set **Global Search** to **False**.
5. Click **Done**.
6. Click  > **Solution Configuration** > **Object Types**.
7. Select the object type labeled **Risk** with the name **SOXRisk**.
8. Under **Field Groups**, click **OPSS-Rsk**.
9. Click **Owner**.
10. Scroll down and set **Global Search** to **False**.
11. Click **Done**.
12. Click  > **System Configuration** > **Global Search** and click **Create**.

Create appears only on initial enablement.

Creating the index also enables global search.

Example: adding or removing object types and fields with an already-enabled global search

After global search is enabled, you can add or remove object types and fields.

About this task

This example assumes that you have enabled global search based on the example in “[Example: customizing global search on initial enablement](#)” on page 524. You now need to make changes such as adding to global search the object type **SOXSubaccount** and the field **Owner** of the object type **SOXRisk** so they are searchable. This example also assumes that you want to remove the field **Additional Description** from the field group of **MRG-BusEnt** of the object type **SOXBusEntity**.

Procedure

1. Log in to IBM OpenPages with Watson with administrative privileges.
2. Click  > **Solution Configuration** > **Object Types**.
3. Select the object type labeled **Sub-Account** with the name **SOXSubaccount**.
4. Click **Edit** and set **Global Search** to **True**.
5. Click **Save**.
6. Click  > **Solution Configuration** > **Object Types**.
7. Select the object type labeled **Risk** with the name **SOXRisk**.
8. Under **Field Groups**, click **OPSS-Rsk**.
9. Click **Owner**.
10. Scroll down and set **Global Search** to **True**.
11. Click **Done**.
12. Click  > **Solution Configuration** > **Object Types**.
13. Select the object type labeled **Business Entity** with the name **SOXBusEntity**.
14. Under **Field Groups**, click **MRG-BusEnt**.
15. Click **Additional Description**.
16. Scroll down and set **Global Search** to **False**.
17. Click **Done**.
18. Click  > **System Configuration** > **Global Search** and click **Check for Updates**.
19. Click **Update** to start an update operation so that your global search index is synced with the changes you made.

Global search is now updated and ready for use. During the **Update** operation, global search is offline. Any user who attempts to use global search receives a message to this effect. Plan an update during off-hours, and communicate the scheduling of the update to your users.

Changing the database connection information for the search server

You can change the connection information that the search server uses to access the database server.

Procedure

1. Disable global search and stop the global search services.

For more information, see “[Stopping the global search services by using a script](#)” on page 713 or “[Stopping the global search services](#)” on page 715.

2. Log on to the search server as a user with administrative privileges.
3. Go to <SEARCH_HOME>/OPSearch/opsearchtools/.
4. Open the openpages_search.properties file in a text editor.
5. Modify the database connection properties to meet the needs of your environment.

Use the following examples as a guide.

IBM Db2

```
# Database connectivity information
OPSearchTool.DatabaseType = DB2
OPSearchTool.DbaseHostName = OP73-WIN-DB2
OPSearchTool.DatabasePort = 50000
OPSearchTool.DatabaseName = OPX
OPSearchTool.DatabaseUserID = openpages_db_user_id
OPSearchTool.DatabasePassword = openpages_db_password
```

Oracle

```
# Database connectivity information
OPSearchTool.DatabaseType = Oracle
OPSearchTool.DbaseHostName = OP73-WIN-ORACLE
OPSearchTool.DatabasePort = 1521
OPSearchTool.DatabaseName = OPX
OPSearchTool.DatabaseUserID = openpages_db_user_id
OPSearchTool.DatabasePassword = openpages_db_password
```

6. Encrypt the database password in the search properties file.

The database password that you entered in the openpages_search.properties file is in plain text. Change the password to encrypt it. For more information, see “[Setting login information for the search server](#)” on page 518.

7. Start the global search services.

For more information, see one of the following topics:

- “[Starting the global search services by using a script](#)” on page 712
- “[Starting the global search services on Windows](#)” on page 713
- “[Starting the global search services on Linux](#)” on page 714

Displaying a custom field in global search results

The administrator can configure one additional custom field to be displayed in the search results for each object type.

About this task

By default, search results return the Name, Description, and Folder Path field values. For some object types, those fields might not contain enough details about the record to help users determine whether the record they are looking for is in the search result. As administrator, you can customize global search results to contain one additional field in the search results to help users.

This additional field is configured globally across profiles.

The additional field supports text area and text box display types only. If any other display type is used, the search results might not display the field value correctly.

Procedure

1. Log on to OpenPages with Watson as a user with administrative privileges.
2. Click  > **System Configuration** > **Settings**.

3. Click **Platform > Search > Result Fields**

4. Locate the object type for which you want to add an additional field to the search result.

If the object type for which you want to add the additional field is not listed, select **Result Fields** by clicking the check box next to it, and then click **New Setting** to create it.

5. Select the setting for which you want to add additional field for that object type.

6. Set or change the value by using the following format: *Field-Group.Field-Name*.

The additional field value appears after the Description system field on a new line in the items returned from a global search. For example, OPSS-LossEv.What Happened displays the text of the field What Happened in the search result. If the field does not have any value, the field name is shown in the result, but with no value.



Attention: You must provide the correct field group and field name for the additional field.

If the formatting is wrong, or if the field group or field name do not match what is in your OpenPages schema, that additional field is not included in the search results.

You can ensure that you use the correct field group and field name by going to the source. For example, to add a field to search results for the Workpaper object type:

a. Log on to OpenPages with Watson as a user with administrative privileges.

b. Select your object type. Click

c. Select **Workpaper**.

d. Select your field-group. From **Field Groups**, click the field group **OPSS-Work**.

e. Select your field-name. From **Fields**, find the name of the custom field you want to add. For example, **Audit Description**.

f. Make sure that you have the field group and field name correct, for example, OPSS-Work.Audit Description. Follow the steps in the preceding procedure. For example, click > **System Configuration > Settings**.

g. Click **Platform > Search > Result Fields > Workpaper**.

h. Set or change the value to OPSS-Work.Audit Description and click **Done**. The additional field value Audit Description appears after the Description system field on a new line in the items that are returned from a global search.

Global search settings

You can tune and customize global search to suit your organizational needs and policies.

Some settings are already optimized and do not need any changes. Some are preset on initial installation of IBM OpenPages with Watson. And some require attention if you make changes to global search. This section lists the available settings for global search, with a summary of what they do, and explains when you might need to make changes to settings.

There are also search properties that are not specified in settings. For more information, see “[The global search properties file](#)” on page 538.



Attention: Where you are told “Do not need to modify this setting unless you are instructed to do so by customer support”, do not modify the setting without consulting first with IBM OpenPages Support. Changing these settings can result in global search not working or unexpected performance issues.

Many global search settings are set as hidden by default. You must unhide them first. For more information, see “[Unhiding the hidden global search settings](#)” on page 527.

Unhiding the hidden global search settings

Many global search settings are set as hidden by default. Before you can change the global search settings, you must unhide them.

Procedure

1. Log in to IBM OpenPages with Watson with administrative privileges.
2. Click  > **System Configuration** > **Settings**.
3. Click **Applications** > **Common** > **Configuration** and select **Show Hidden Settings**.
4. Change the value from **false** to **true**.

You can now see all of the settings in your IBM OpenPages with Watson environment.

Setting the Query Path to the global search administration server

Specifies the query path to the search server that handles administration.

Procedure

1. Log in to IBM OpenPages with Watson with administrative privileges.
2. Click  > **System Configuration** > **Settings**.
3. Click **Platform** > **Search** > **Admin** > **Query Path**.
4. Change the value as required.



Attention: Do not modify this setting unless you are instructed by IBM OpenPages Support to do so. Changing this setting can result in global search not working or unexpected performance issues.

Setting the URL to the global search administration server

Specifies the URL path to the IBM OpenPages global search server that handles administration.

About this task

The value of this setting is set based on your initial installation of global search. If you decide to reinstall global search on a different server, or enable SSL, or select a different port value, you must make the appropriate change. If you enable SSL, then change `http` to `https`. If you change the server on which global search is installed, you must provide the server hostname or the IP address. If you need to use a different port other than the default, you must specify the different port.



Attention: Before you change this setting, make sure that global search is disabled. For more information, see [“Enabling and disabling global search” on page 521](#).

Procedure

1. Log in to IBM OpenPages with Watson with administrative privileges.
2. Click  > **System Configuration** > **Settings**.
3. Click **Platform** > **Search** > **Admin** > **Search Server Administration URL**.
4. Change the value as required.



Attention: If you are changing this setting because you want to enable SSL or because you want to change the server on which global search is installed, then you must also make the same change to the settings **Platform** > **Search** > **Index** > **Search Server URL** and **Platform** > **Search** > **Request** > **Search Server URL**.

Setting the progress refresh interval

Specifies the frequency (in seconds) of updating progress in the IBM OpenPages with Watson.

Procedure

1. Log in to IBM OpenPages with Watson with administrative privileges.
2. Click  > **System Configuration** > **Settings**.
3. Click **Platform** > **Search** > **Index** > **Full** > **Progress Refresh Interval**.
4. Change the value as required. The default value is 30 seconds.



Attention: Do not modify this setting unless you are instructed by customer support to do so. Changing this setting can result in global search not working or unexpected performance issues.

Setting the number of records to cache

Specifies the total number of records to cache before sending to the Apache Solr server for indexing.

About this task

If you increase the value of this setting, the initial full index might take less time, depending on your system configuration and database provider. However, this might require more RAM, CPU, and network resources. See the section on global search properties on how to increase the available memory to offset out-of-memory issues if you make a change to this setting.

Procedure

1. Log in to IBM OpenPages with Watson with administrative privileges.
2. Click  > **System Configuration** > **Settings**.
3. Click **Platform** > **Search** > **Index** > **Full** > **Record Cache Size**.
4. Change the value as required. The default value is 100.



Attention: Do not modify this setting unless you are instructed by IBM OpenPages Support to do so. Changing this setting can result in global search not working or unexpected performance issues.

Setting the polling interval

Specifies the polling interval (in seconds) to check for changes (added, modified, or deleted) in IBM OpenPages with Watson objects.

About this task

By default, global search checks every minute if your data changes in the IBM OpenPages with Watson database. If the database contains changes, global search syncs up the search index so that when users search, those changes are reflected in the search result.

Reducing the polling interval means that the search index is more in sync with the database changes. However, this might result in slower database performance that impacts other IBM OpenPages with Watson operations, as well as slower search performance due to more frequent updates. Based on the load of your system and available resources, you might find you must increase this value to 300 (5 minutes) to offset the load. If you change this value, you must disable and then enable global search for the change to take effect. For more information, see [“Enabling and disabling global search” on page 521](#).

Procedure

1. Log in to IBM OpenPages with Watson with administrative privileges.
2. Click  > **System Configuration** > **Settings**.
3. Click **Platform** > **Search** > **Index** > **Incremental** > **Polling Interval**.

4. Change the value as required. The default value is 60.

Setting the number of records to cache before sending to the server for indexing

Specifies the total number of records to cache before sending to the Apache Solr server for indexing.

About this task

If you increase the value of this setting, the initial full index might take less time, depending on your system configuration and database provider. However, this might require more RAM, CPU, and network resources. See the section on global search properties on how to increase the available memory to offset out-of-memory issues if you change this setting.

Procedure

1. Log in to IBM OpenPages with Watson with administrative privileges.
2. Click  > **System Configuration** > **Settings**.
3. Click **Platform** > **Search** > **Index** > **Incremental** > **Record Cache Size**.
4. Change the value as required. The default value is 100.



Attention: Do not modify this setting unless you are instructed by IBM OpenPages Support to do so. Changing this setting can result in global search not working or unexpected performance issues.

Setting the Query Path to the Apache Solr server that handles Folder ACL indexing

Specifies the URL path to the Apache Solr server that handles Folder ACL indexing.

Procedure

1. Log in to IBM OpenPages with Watson with administrative privileges.
2. Click  > **System Configuration** > **Settings**.
3. Click **Platform** > **Search** > **Index** > **Folder ACL Query Path**.
4. Change the value as required.



Attention: Do not modify this setting unless you are instructed by customer support to do so. Changing this setting can result in global search not working or unexpected performance issues.

Setting the language analyzer that is used by search

Specifies the two or three letter abbreviation for the language analyzer that is used by search, that is, the language that search is optimized for.

Before you begin

If global search is already enabled, disable global search and drop the current index. For more information, see [“Enabling and disabling global search” on page 521](#).

About this task

Search results might be of different quality for other languages. For best results, use one of the supported locale languages: en=English (US or UK), pt=Brazilian Portuguese, fr=French, de=German, it=Italian, ja=Japanese, es=Spanish, cjk=Chinese, Japanese, Korean, zh=Simplified Chinese.

The value of this setting is set based on your initial installation of global search. If after installing global search you decide to change the language locale of your database data, you must modify the value of this setting to reflect the language of your text. If your data has mixed language text, such as English and Chinese, pick the language in which most of your data is created; this language becomes the main language for which global search is optimized.

Procedure

1. Log in to IBM OpenPages with Watson with administrative privileges.
2. Click  > **System Configuration** > **Settings**.
3. Click **Platform** > **Search** > **Index** > **Language Analyzer**.
4. Change the value as required. The default value is **en**.



Attention: Before you make a change to this setting, if global search is already enabled, make sure to disable global search and drop the current index. For more information, see “[Enabling and disabling global search](#)” on page 521.

Setting the Query Path to the Apache Solr server that handles Folder ACL indexing

Specifies the URL path to the Apache Solr server that handles indexing.

Procedure

1. Log in to IBM OpenPages with Watson with administrative privileges.
2. Click  > **System Configuration** > **Settings**.
3. Click **Platform** > **Search** > **Index** > **Query Path**.
4. Change the value as required.



Attention: Do not modify this setting unless you are instructed by customer support to do so. Changing this setting can result in global search not working or unexpected performance issues.

Setting the URL to the Apache Solr server that handles Folder ACL indexing

Specifies the URL for the search server index.

About this task

The value of this setting is set based on your initial installation of global search. If you decide to reinstall global search on a different server, or enable SSL, or select a different port value, you must make the appropriate change. If you enable SSL, then change http to https. If you change the server on which global search is installed, you must provide the server hostname or the IP address. If you need to use a different port other than the default, you must specify the different port



Attention: Before you make a change to this setting, make sure that global search is disabled. For more information, see “[Enabling and disabling global search](#)” on page 521.

Procedure

1. Log in to IBM OpenPages with Watson with administrative privileges.
2. Click  > **System Configuration** > **Settings**.
3. Click **Platform** > **Search** > **Index** > **Search Server URL**.
4. Change the value as required.



Attention: If you are changing this setting because you want to enable SSL or because you want to change the server on which global search is installed, then you must also make the same change to the settings **Platform > Search > Admin > Search Server Administration URL** and **Platform > Search > Request > Search Server URL**.

Setting the number of records inserted per batch

Specifies the number of search results records that are inserted per batch.

Procedure

1. Log in to IBM OpenPages with Watson with administrative privileges.
2. Click  > **System Configuration > Settings**.
3. Click **Platform > Search > Request > Batch Size**.
4. Change the value as required. The default value is 1000.



Attention: Do not modify this setting unless you are instructed by customer support to do so. Changing this setting can result in global search not working or unexpected performance issues.

Setting the Query Path to the Apache Solr server that handles Folder ACL search requests

Specifies the URL path to the Apache Solr server that handles Folder ACL search requests.

Procedure

1. Log in to IBM OpenPages with Watson with administrative privileges.
2. Click  > **System Configuration > Settings**.
3. Click **Platform > Search > Request > Folder ACL Query Filter**.
4. Change the value as required.



Attention: Do not modify this setting unless you are instructed by customer support to do so. Changing this setting can result in global search not working or unexpected performance issues.

Setting the URL to the Apache Solr server that handles OpenPages search requests

Specifies the URL path to the Apache Solr server that handles search requests.

Procedure

1. Log in to IBM OpenPages with Watson with administrative privileges.
2. Click  > **System Configuration > Settings**.
3. Click **Platform > Search > Request > Query Path**.
4. Change the value as required.



Attention: Do not modify this setting unless you are instructed by customer support to do so. Changing this setting can result in global search not working or unexpected performance issues.

Setting the number of attempts to fill the search results

Specifies the number of attempts to fill the search results defined in **Search Page Size** with viewable records after security is applied on **Result Cache Size** items.

Procedure

1. Log in to IBM OpenPages with Watson with administrative privileges.
2. Click  > **System Configuration** > **Settings**.
3. Click **Platform** > **Search** > **Request** > **Result Cache Refill Attempts**.
4. Change the value as required. The default value is 5.



Attention: Do not modify this setting unless you are instructed by customer support to do so. Changing this setting can result in global search not working or unexpected performance issues.

Setting the number of search results records that are cached per user session

Specifies the number of search results records that are cached per user session. This value sets the upper limit for the number of results that are shown to the user.

Procedure

1. Log in to IBM OpenPages with Watson with administrative privileges.
2. Click  > **System Configuration** > **Settings**.
3. Click **Platform** > **Search** > **Request** > **Result Cache Size**.
4. Change the value as required. The default value is 100.



Attention: Do not modify this setting unless you are instructed by customer support to do so. Changing this setting can result in global search not working or unexpected performance issues.

Setting the internal page size for search results

Specifies a two-number value that controls the total number of results that Apache Solr returns.

About this task

Results that come back from Solr are post processes, and only those results that meet the security rules of the user are kept and presented to the user. If a user has a restrictive security rule and policy, it is possible that most of what is in the initial page of 500 items might be eliminated in an attempt to fill the cache setting that is specified in **Platform** > **Search** > **Request** > **Result Cache Size**. If so, an additional 10,000 items are retired from Apache Solr and are post processed.

If your organization uses a complex security model, and many of your users have restrictive security rules and policies, chances are they see fewer results than expected. Advise those users to refine their search terms. You can also help users by increasing the value of this setting. Increasing the value of this setting might impact search performance.

Procedure

1. Log in to IBM OpenPages with Watson with administrative privileges.
2. Click  > **System Configuration** > **Settings**.
3. Click **Platform** > **Search** > **Request** > **Search Page Size**.

4. Change the value as required. The default value is 500|10000.



Attention: Do not modify this setting unless you are instructed by IBM OpenPages Support to do so. Changing this setting can result in global search not working or unexpected performance issues.

Setting the URL to the Apache Solr server that handles search requests

Specifies the URL for search requests.

About this task

The value of this setting is set based on your initial installation of global search. If you decide to reinstall global search on a different server, or enable SSL, or select a different port value, you must make the appropriate change. If you enable SSL, then change http to https. If you change the server on which global search is installed, you must provide the server hostname or the IP address. If you need to use a different port other than the default, you must specify the different port

Attention: Before you change this setting, make sure that global search is disabled. For more information, see [“Enabling and disabling global search” on page 521](#).

Procedure

1. Log in to IBM OpenPages with Watson with administrative privileges.
2. Click > **System Configuration** > **Settings**.
3. Click **Platform** > **Search** > **Request** > **Search Server URL**.
4. Change the value as required.



Attention: If you are changing this setting because you want to enable SSL or because you want to change the server on which global search is installed, then you must also make the same change to the settings **Platform** > **Search** > **Admin** > **Search Server Administration URL** and **Platform** > **Search** > **Index** > **Search Server URL**.

Setting a time limit to search before timing out

Specifies the approximate time (in milliseconds) for Apache Solr to search before timing out.

Procedure

1. Log in to IBM OpenPages with Watson with administrative privileges.
2. Click > **System Configuration** > **Settings**.
3. Click **Platform** > **Search** > **Request** > **Search Timeout**.
4. Change the value as required. The default value is 60000.



Attention: Do not modify this setting unless you are instructed by customer support to do so. Changing this setting can result in global search not working or unexpected performance issues.

Setting an additional field in the search result set

s Specifies an additional field for an object type to be returned as part of the search result set.

Procedure

1. Log in to IBM OpenPages with Watson with administrative privileges.
2. Click > **System Configuration** > **Settings**.

3. Click **Platform** > **Search** > **Result Fields** > **<object type name>**.
4. If the object type for which you want to add the additional field is not on the list, you can create a new setting for it. Select the **Result Fields** node, and then click **New Setting**.
5. For details on how to change or provide a new value, see “[Displaying a custom field in global search results](#)” on page 526.

Setting whether to allow compression

Specifies whether the data being passed between the Apache Solr server and IBM OpenPages with Watson is compressed.

Procedure

1. Log in to OpenPages with administrative privileges.
2. Click  > **System Configuration** > **Settings**.
3. Click **Platform** > **Search** > **Allow Compression**.
4. Change the value as required. The default value is **true**.



Attention: Do not modify this setting unless you are instructed to do so by customer support. Changing this setting can result in global search not working or unexpected performance issues.

Setting the network connection request timeout

Specifies the network connection request timeout (in milliseconds) to the Apache Solr server.

Procedure

1. Log in to IBM OpenPages with Watson with administrative privileges.
2. Click  > **System Configuration** > **Settings**.
3. Click **Platform** > **Search** > **Connection Timeout**.
4. Change the value as required. The default value is 5000.



Attention: Do not modify this setting unless you are instructed by customer support to do so. Changing this setting can result in global search not working or unexpected performance issues.

Setting whether to allow URL redirects

Specifies whether URL redirects are allowed.

Procedure

1. Log in to IBM OpenPages with Watson with administrative privileges.
2. Click  > **System Configuration** > **Settings**.
3. Click **Platform** > **Search** > **Follow Redirects**.
4. Change the value as required. The default value is **false**.



Attention: Do not modify this setting unless you are instructed by customer support to do so. Changing this setting can result in global search not working or unexpected performance issues.

Setting the number of allowed connections from the platform

Specifies the number of allowed connections to the Apache Solr server from IBM OpenPages with Watson.

Procedure

1. Log in to OpenPages with administrative privileges.
2. Click  > **System Configuration** > **Settings**.
3. Click **Platform** > **Search** > **Maximum Connections Per Host**.
4. Change the value as required. The default value is 100.



Attention: Do not modify this setting unless you are instructed to do so by customer support. Changing this setting can result in global search not working or unexpected performance issues.

Setting the number of allowed connections

Specifies the total number of allowed connections to the Apache Solr server.

Procedure

1. Log in to IBM OpenPages with Watson with administrative privileges.
2. Click  > **System Configuration** > **Settings**.
3. Click **Platform** > **Search** > **Maximum Total Connections**.
4. Change the value as required. The default value is 1000.



Attention: Do not modify this setting unless you are instructed by customer support to do so. Changing this setting can result in global search not working or unexpected performance issues.

Setting the number of times a request is reattempted

On error, specifies the number of times a request is reattempted before reporting a request failure.

Procedure

1. Log in to IBM OpenPages with Watson with administrative privileges.
2. Click  > **System Configuration** > **Settings**.
3. Click **Platform** > **Search** > **Request Retry Attempts**.
4. Change the value as required. The default value is 3.



Attention: Do not modify this setting unless you are instructed by customer support to do so. Changing this setting can result in global search not working or unexpected performance issues.

Setting the socket timeout for indexing

Specifies the socket connection timeout (in milliseconds) to the Apache Solr server for indexer use.

Procedure

1. Log in to IBM OpenPages with Watson with administrative privileges.
2. Click  > **System Configuration** > **Settings**.
3. Click **Platform** > **Search** > **Socket Timeout (index)**.

4. Change the value as required. The default value is 1800000.



Attention: Do not modify this setting unless you are instructed by customer support to do so. Changing this setting can result in global search not working or unexpected performance issues.

Setting the socket timeout for searching

Specifies the socket connection timeout (in milliseconds) to the Apache Solr server for search use.

Procedure

1. Log in to IBM OpenPages with Watson with administrative privileges.
2. Click > **System Configuration** > **Settings**.
3. Click **Platform** > **Search** > **Socket Timeout (search)**.
4. Change the value as required. The default value is 5000.



Attention: Do not modify this setting unless you are instructed by customer support to do so. Changing this setting can result in global search not working or unexpected performance issues.

Setting the Apache Solr password

Specifies the Apache Solr password to authenticate against the user ID.

Procedure

1. Log in to IBM OpenPages with Watson with administrative privileges.
2. Click > **System Configuration** > **Settings**.
3. Click **Platform** > **Search** > **Solr Password**.
4. Change the value as required. The default value is encrypted text.



Attention: Do not modify this setting unless you are instructed by customer support to do so. Changing this setting can result in global search not working or unexpected performance issues.

Setting the Apache Solr user ID

Specifies the Apache Solr user ID to authenticate against the server.

Procedure

1. Log in to IBM OpenPages with Watson with administrative privileges.
2. Click > **System Configuration** > **Settings**.
3. Click **Platform** > **Search** > **Solr User ID**.
4. Change the value as required. The default value is 0.



Attention: Do not modify this setting unless you are instructed by customer support to do so. Changing this setting can result in global search not working or unexpected performance issues.

Setting the default number of search results to return per page

Specifies the default number of search results to return per page.

Procedure

1. Log in to IBM OpenPages with Watson with administrative privileges.
2. Click  > **System Configuration** > **Settings**.
3. Click **Applications** > **GRCM** > **Search** > **Default Results Page Size**.
4. Change the value as required. Allowable values are **10**, **25**, and **50**. The default value is **10**.



Attention: If you change the value of this setting to a value larger than 10, global search and the overall performance OpenPages might be impacted. This change is global to all users.

The global search properties file

To customize global search, you can specify properties in the global search properties file.

The property file is named `openpages_search.properties`, and is located in `<SEARCH_HOME>/OPSearch/opsearchtools/`. If you make changes to this file, you must disable and then enable global search for the change to take effect. For more information, see [“Enabling and disabling global search” on page 521](#).

Some changes might require you to drop the global search index and re-create it.

Most properties in this file are set to the default value. Only those properties that you might need to interact with are documented; the rest must not be modified unless you are instructed to do so by IBM OpenPages Support.

You can also use settings to tune and customize global search. For information about specifying the settings, see [“Global search settings” on page 527](#).

Setting the error handling parameters for the indexer

Use this property to set error handling parameters for the indexer that it might run into.

About this task

During indexing (both full and incremental) the indexer can run into issues such as bad records, database errors, network issues, and so on. If so, the indexer attempts to recover from those issues and continue indexing instead of ending. It does so by entering an error-handler mode, indexing until it recovers from the error or reaches a number of retries. Those parameters are set by using four values of **Major**, **Minor**, **Panic**, and **PanicLimit**.

By default, indexing is performed on an object type by processing all records in that object type in one continuous process. If an error is encountered, the indexer enters an error-handler mode. In this mode, it processes a chunk of 100 records (the value for **Major**) at a time. If it still runs into an issue, it scales back to a chunk of 10 records (the value for **Minor**) and if it still runs into an issue, it scales back to a chunk of one record (the value for **Panic**). If it still runs into issues, it attempts up to **PanicLimit** times before giving up and skipping that record from the index, and it goes back to the chunk of **Major** after which it goes back to normal indexing without chunking.

Procedure

1. Log in to IBM OpenPages with Watson with administrative privileges.
2. Go to the `<SEARCH_HOME>/OPSearch/opsearchtools/` folder.
3. Open the `openpages_search.properties` file.
4. Change the **OPSearchTool.IndexerErrorHandlerParameters** property as required.



Attention: If you change to the `openpages_search.properties` file, you must disable and then enable global search for the change to take effect. For more information, see [“Enabling and disabling global search” on page 521](#).

Setting the maximum opsearchtool.jar heap size

Use this property to set the maximum heap size, in megabytes, to be used by opsearchtool.jar for general operations.

About this task

You might need to increase the value of the **OPSearchTool.SearchToolHeapSize** property if you encounter out-of-memory issues during general opsearchtool.jar operations. The out-of-memory issues might be due to the complexity of an OpenPages schema that contains many profiles, object types, field groups, and fields.

Procedure

1. Log in to IBM OpenPages with Watson with administrative privileges.
2. Go to the <SEARCH_HOME>/OPSearch/opsearchtools/ folder.
3. Open the openpages_search.properties file.
4. Change the **OPSearchTool.SearchToolHeapSize** property as required.



Attention: If you change to the openpages_search.properties file, you must disable and then enable global search for the change to take effect. For more information, see [“Enabling and disabling global search” on page 521](#).

Setting the maximum Apache Solr heap size

Use this property to set the maximum heap size, in megabytes, to be used by Apache Solr.

About this task

You might need to increase the value of the **OPSearchTool.SolrHeapSize** property if you encounter out-of-memory issues while indexing or searching. The out-of-memory issues might be due to the size of your records or the number of records that are indexed.

If you increase the heap size and you do not have sufficient free memory on the system, you might cause further out-of-memory issues and experience performance issues with global search.

Procedure

1. Log in to IBM OpenPages with Watson with administrative privileges.
2. Go to the <SEARCH_HOME>/OPSearch/opsearchtools/ folder.
3. Open the openpages_search.properties file.
4. Change the **OPSearchTool.SolrHeapSize** property as required.



Attention: If you change to the openpages_search.properties file, you must disable and then enable global search for the change to take effect. For more information, see [“Enabling and disabling global search” on page 521](#).

Setting the maximum opsearchtool.jar heap size during indexing

Use this property to set the maximum heap size, in megabytes, to be used by the opsearchtool.jar file during indexing.

About this task

You might need to increase the value of the **OPSearchTool.IndexerHeapSize** property if you run into out-of-memory issues during full indexing or incremental indexing.

The out-of-memory issues might be due to the size of your records that are indexed.

If you increase the heap size and you do not have sufficient free memory on the system, you might cause further out-of-memory issues and experience performance issues with global search.

Procedure

1. Log in to IBM OpenPages with Watson with administrative privileges.
2. Go to the <SEARCH_HOME>/OPSearch/opsearchtools/ folder.
3. Open the openpages_search.properties file.
4. Change the **OPSearchTool.IndexerHeapSize** property as required.



Attention: If you change to the openpages_search.properties file, you must disable and then enable global search for the change to take effect. For more information, see “[Enabling and disabling global search](#)” on page 521.

Setting the maximum text extraction heap size for indexing

The **OPSearchTool.TextExtractorHeapSize** is used to handle the indexing of file attachments when the amount of extracted text is large. The property sets the maximum heap size, in megabytes, to use. Once the total is reached, the files are immediately added to Solr before adding any others. This property helps to minimize possible memory related issues.

About this task

If you encounter out-of-memory issues during full indexing or incremental indexing, increase the value of the **OPSearchTool.TextExtractorHeapSize** property. The out-of-memory issues might be due to the size and complexity of your file attachments.

If you do not have sufficient free memory on the system for the heap size that you configured, you might cause further out-of-memory issues and experience performance issues with global search.

Procedure

1. Log in to IBM OpenPages with Watson with administrative privileges.
2. Go to the <SEARCH_HOME>/OPSearch/opsearchtools/ folder.
3. Open the openpages_search.properties file.
4. Change the **OPSearchTool.TextExtractorHeapSize** property as required.



Attention: If you change to the openpages_search.properties file, you must disable and then enable global search for the change to take effect. For more information, see “[Enabling and disabling global search](#)” on page 521.

Setting the text extractor timeout limit

Use this property to limit how long, in milliseconds, to wait for the text extractor to extract text from file attachments during indexing.

About this task

You might need to increase the value of the **OPSearchTool.TextExtractorTimeout** property during full indexing or incremental indexing.

The timeout issues might be due to the size and complexity of your file attachments or the limits of your overall system performance.

Procedure

1. Log in to IBM OpenPages with Watson with administrative privileges.
2. Go to the <SEARCH_HOME>/OPSearch/opsearchtools/ folder.

3. Open the openpages_search.properties file.
4. Change the **OPSearchTool.TextExtractorTimeout** property as required.



Attention: If you change to the openpages_search.properties file, you must disable and then enable global search for the change to take effect. For more information, see “[Enabling and disabling global search](#)” on page 521.

Setting the maximum text to extract from file attachments for indexing

Use this property to set the maximum text string, in megabytes, to extract from file attachments for indexing.

About this task

The **OPSearchTool.FileExtractionSize** property helps to prevent out-of-memory errors during the indexing of large file attachments.

By default, the maximum text string that is extracted from file attachments for indexing is 500 MB.

If you increase the value of the **OPSearchTool.FileExtractionSize** property, the indexing process might run more quickly but you might encounter out-of-memory issues during full indexing or incremental indexing.

If you decrease the value, the indexing process runs more slowly but you might avoid the out-of-memory issues.

Procedure

1. Log in to IBM OpenPages with Watson with administrative privileges.
2. Go to the <SEARCH_HOME>/OPSearch/opsearchtools/ folder.
3. Open the openpages_search.properties file.
4. Change the **OPSearchTool.FileExtractionSize** property as required.



Attention: If you change to the openpages_search.properties file, you must disable and then enable global search for the change to take effect. For more information, see “[Enabling and disabling global search](#)” on page 521.

Setting the root path location for file attachment search

Use this property to set the file storage root path location for file attachment search.

About this task

When OpenPages search server is on a different server than the OpenPages application server, the search server must have access to the OpenPages file storage location in order for it to index file attachments. If the search server is on a Windows operating system, you can use either the Uniform Naming Convention (UNC) or Local File System (LFS) path. If the search server is on a Linux operating system, you must use the LFS path.

Windows UNC path example:

\\\OPAppServer\shared\OpenPages\openpages-storage

Windows FLS path example:

C:\shared\OpenPages\openpages-storage

Linux FLS path example:

/shared/OpenPages/openpages-storage



Attention: You must double the “\” character in the UNC and FLS path on Windows, otherwise the path is not properly processed.

Procedure

1. Log in to IBM OpenPages with Watson with administrative privileges.
2. Go to the <SEARCH_HOME>/OPSearch/opsearchtools/ folder.
3. Open the openpages_search.properties file.
4. Change the **OPSearchTool.FileStorageRootPath** property as required.

Global search FAQs

Questions are sometimes asked about global search and how it works.

Global search indexing

Q. How does the indexing work?

A. IBM OpenPages global search server includes an indexing service. When you click **Create** in the Administration UI, the indexing service queries the OpenPages database for records of object types and fields that are enabled for global search. Those records are read, formatted, and then indexed by Apache Solr. The index is later used for search when the global search feature is used from the OpenPages UI.

This one-time initial indexing is called full indexing. After full indexing is complete, the global search indexer service enters an incremental indexing mode. Incremental indexing mode queries the OpenPages database once a minute for modified records, newly added records, or deleted records of object types that are enabled for global search and reindexes them to keep the global search index in sync with the OpenPages data.

Q. Does global search crawl the network-attached storage (NAS) (openpages-storage location)?

A. OpenPages uses file storage, and shares the file storage location across all instances of OpenPages applications. By default, OpenPages global search is configured with file search enabled. So yes, if file search is enabled, access to openpages-storage location must be set for global search. For more information, see [“Setting the root path location for file attachment search” on page 541](#).

Q. Are there any regularly scheduled batch jobs?

A. Yes, there is a regularly scheduled batch job that runs. The indexer (when it is running in incremental indexing mode) runs as a regularly scheduled batch job.

Q. Are the indexes and logs stored on a local drive?

A. OpenPages global search index is a proprietary format of Apache Solr, and is stored on the local hard disk drive where the global search server is installed. OpenPages global search can be installed on any local hard disk drive on the system where you installed global search. For optimal performance, it is best to install global search on a separate solid-state drive, that is, not on the same drive as the operating system.

Q. How is the index used by the product?

A. The index is proprietary to Apache Solr, is used by Apache Solr only, and is stored on the local file system where global search is installed. The index is accessed and updated anytime global search is indexing in both full and incremental mode, and the index is looked up anytime an OpenPages user is running a search using global search.

Q: How do I drop and re-create the index?

For information about dropping and re-creating the index, see [“Recreating the index for global search” on page 522](#).

Sizing and scaling

Q. The documentation mentions that global search can be run only as a single instance.

A. This is correct. A single instance of OpenPages global search server can handle all search requests from all OpenPages application servers.

Q. Can a single search server be shared by multiple environments, such as Development, Testing, Staging, or Production?

A. No. Each environment must have its own OpenPages global search server.

Q. We have two application servers and two Cognos servers for staging and production; do we need to have two global search servers?

A. A single OpenPages global search server works with all OpenPages application servers and Cognos servers. It is strongly recommended to have a separate global search server for staging and production.

Q. Is there a possibility of running global search when using F5 load balancing in an active-active scenario?

A. Because there is only a single instance of OpenPages global search server, there is no need for F5 load balancing.

Q. How does global search impact the database server?

A. During full indexing mode, the database server is used to serve records to the global search indexer. The same is true during incremental indexing mode, but the load on the database is less because only modified records and newly added records are read. When a user uses global search and complex security rules exist for that user, those rules are processed, so the complexity of the rules determines the impact on the database server.

Q. Do we have any metrics for indexing volumes? What is the speed? Do we have any indicative query response times?

A. There are several factors influence the indexing volume and duration. The number of object types and their fields you enabled for global search and the total number of records, as well as the data size in those records in your database, all influence how long it takes to complete the initial full indexing and how large the index size on disk is. Query response time is within seconds for most searches. In some cases, if a user has complex security rules, it's possible a search can take more than several seconds.

High Availability (HA) and Disaster Recovery (DR)

Q. We have two application servers; one acts as an active administration server and the other one is a passive disaster recovery (DR) server. Do the global search servers also need to be active and passive?

A. No. Because there is only one instance of OpenPages global search server, there is no active / passive setup for it.

Q. Indexing can be lost in a DR scenario. In a DR scenario, does global search require reindexing?

A. Yes. This requires you to fully reindex for the global search feature to become available again. However, all other OpenPages functionality continues to work as normal while the global search index is being re-created.

Maintenance

Q. Are there any backup and restore operations to be performed on the global search server?

A. There are no backup and restore requirements for OpenPages global search. However, if you restore the database from a backup, the global search index is now out of sync with the OpenPages database. In this scenario, you must re-create the global search index by first disabling global search, then dropping the index, and then creating the index.

Q. Are there any index optimizations?

A. There is no need to optimize the OpenPages global search index. Apache Solr dynamically and automatically optimizes the index over time. If you perform a bulk update that impacts over 50% of your records and you have many records - hundreds of thousands of records, for example - the automatic index optimization of Apache Solr can take several days to catch up. If you suspect search performance is suffering because of a bulk update, you can force an index optimization from the Apache Solr administration page.

Collecting search diagnostic data

See [“Before you contact IBM OpenPages Support” on page 945](#).

Chapter 22. Using IBM OpenPages with Watson utilities with Db2 databases

You can use the IBM OpenPages with Watson utilities to back up and restore the OpenPages and Cognos files and configuration data.

Use the utilities that are provided with IBM Db2 to back up and restore databases in IBM OpenPages with Watson.

Db2 and the OpenPages with Watson backup and restore utilities

The backup and restore utilities are installed during the IBM OpenPages with Watson installation. You can use the utilities to back up and restore the OpenPages with Watson application. The utilities do not back up or restore the databases.

Use the utilities that are provided with IBM Db2 to back up and restore databases in IBM OpenPages with Watson.

For more information about backing up or restoring, see “[Database backup and restore for OpenPages \(Db2\)](#)” on page 555.

For information about developing a database backup and restore strategy, see the [IBM Db2 documentation](#).

Use the following utilities for backing up and restoring the IBM OpenPages application:

- OpenPages with Watson backup (OPBackup) and restore (OPRestore)

These utilities are used to backup and restore the application. For more information, see “[The OPBackup utility \(Db2\)](#)” on page 548. The utilities do not back up or restore the OpenPages with Watson database.

Users can choose to run a live OPBackup. When you run a live OPBackup, OpenPages services are not stopped on the application server, which allows for maximum uptime of the OpenPages application. By default, OpenPages services are restarted.

- Cognos backup (OPCCBackup) and restore (OPCCRestore)

These utilities are used to back up and restore OpenPages with Watson Cognos files. For more information, see “[Using the Cognos Backup utility \(Db2\)](#)” on page 552. The utilities do not back up or restore the Cognos content store.

Configuring backup job notification

You can configure email notification when you complete an IBM OpenPages with Watson application backup or Cognos backup job.

About this task

Log files for email notification are stored in the logs folder in the following locations. A timestamp is included in the log file names.

- For OPBackup (OpenPages with Watson application backup):

`<OP_Home>|aurora|bin|logs`

- For OPCCBackup (Cognos backup):

`<CC_Home>|tools|bin|logs`

Make sure to set rules in your email client to never send emails from the OpenPages with Watson application server to the Spam or Junk mail folders.

Procedure

1. Open a command or shell window and do one of the following.
 - a) For an OPBackup (OpenPages with Watson application backup), navigate to the op-backup-restore.env file in the <OP_HOME>/aurora/bin directory.
 - b) For a OPCCBackup (Cognos backup), navigate to the op-cc-backup-restore.env file in the bin directory where <cc_home> represents the installation of Cognos.
 - For Microsoft Windows, the back up path is OPBackup <path-to-back-up-location>
 - For Linux, the back up path is OpBackup.sh <path-to-back-up-location>where <path-to-backup-location> is the full path of the directory where the backed up files are located on the application server. If a file path is not specified, the OPBackup command uses, by default, the backup location specified in the BACKUP_LOCATION parameter of the <OP_Home> | aurora|bin|op-backup-restore.env file.
2. Open the selected .env file in a text editor.
3. Specify a value after the equal sign (=) for the parameters described in the following table and save the .env file.

Table 163. Backup email parameters

Parameter name	Description
BACKUP_EMAIL_NOTIFICATION_SERVER=	The hostname of the outgoing mail server.
BACKUP_EMAIL_NOTIFICATION_TO_EMAIL_ID=	The name of recipients that will receive the email notification. Separate email addresses with a comma (,). Note: Do not type a comma after the last email address. Example emailid1@yourdomain.com,emailid2@yourdomain.com
BACKUP_EMAIL_NOTIFICATION_FROM_EMAIL_ID=	The name that will appear as the sender of the notification email in the From: field of the email. The email address is also used as the personal name.
BACKUP_EMAIL_NOTIFICATION_SUCCESS_MSG_FILE=BACKUP_SUCCESS_MSG.txt	The BACKUP_SUCCESS_MSG.txt file is the default file containing the message text that will be used if the OPBackup.cmd completes successfully. You can modify the message text in the BACKUP_SUCCESS_MSG.txt file. The first line of the file is used as the email's subject.

Table 163. Backup email parameters (continued)

Parameter name	Description
BACKUP_EMAIL_NOTIFICATION _FAIL_MSG_FILE= BACKUP_FAIL_MSG.txt	The BACKUP_FAIL_MSG.txt file is the default file that contains the message text that is used if the OPBackup.cmd fails with errors. You can modify the message text in the BACKUP_FAIL_MSG.txt file as wanted. The first line of the file is used as the email's subject.

Asynchronous background jobs and administrative functions

IBM OpenPages with Watson supports asynchronous execution of processes in the background.

The most common examples of these types jobs are FastMap web-based data import jobs, object resets, and reporting schema generation.

For example, after a user submits a data import file, that file is queued for loading and the import process occurs in the background. Because it is important for asynchronous background jobs to run to completion, certain administrative operations are suspended until all background jobs complete.

By default, the following administrative functions will not start until background jobs are complete:

- OPBackup command
- OPRestore command
- System Administrative Mode (SAM)

Note: To disable the default setting that checks for background jobs before you start **OPBackup** or **OPRestore**, see [“Enabling and disabling asynchronous background processes checking” on page 548](#).

If asynchronous processes are found, error messages are written to the OPBACKUP restore log. The .log file name has the format op_backup_<yyyy_mm_dd_hh_mm_ss>.log. For example:

- On Windows: C:\OpenPages\openpages-backup-restore\op_backup_2019_07_26_09_35_42.log
- On Linux: /opt/OpenPages/openpages-backup-restore/op_backup_2019_07_26_09_35_42.log

Example

The following samples show the error log message that occurred when an OPBackup command was initiated while the reporting schema was still being generated.

IBM Db2

- For IBM Db2 environments, a sample error log message might look similar to this text:
 - can-proceed:
 [exec] ERROR near line 26:
 [exec] SQL0438N Application raised error or warning with diagnostic
 [exec] text: "There are existing processes running. Please let them
 [exec] finish or termi".
 - can-proceed:
 [exec] ERROR near line 26:
 [exec] SQL0438N Application raised error or warning with diagnostic
 [exec] text: "There are existing object reset operations running.
 [exec] Please let them finish or termi".

Oracle database

For Oracle environments, a sample error log message might look similar to this text:

- can-proceed:
[exec] declare
[exec] *
[exec] ERROR at line 1:
[exec] ORA-20001: There are existing processes running.
[exec] Please let them finish or terminate them before proceeding.
[exec] ORA-06512: at line 7
[exec]
- can-proceed:
[exec] declare
[exec] *
[exec] ERROR at line 1:
[exec] ORA-20001: There are existing object reset operations running.
[exec] Please let them finish or terminate them before proceeding.
[exec] ORA-06512: at line 7
[exec]

Enabling and disabling asynchronous background processes checking

By default, IBM OpenPages with Watson does not allow a backup (OPBackup) or restore (OPRestore) operation to start until all asynchronous background jobs are complete.

It is best to run all jobs to completion before you start a backup or restore operation. However, this check can be enabled or disabled as follows.

Procedure

1. Open a command or shell window on the OpenPages with Watson server.
2. Navigate to the op-backup-restore.env file in the <OP_Home>/aurora/bin directory.
3. Open the op-backup-restore.env file in a text editor.
4. Set the CHECK_BACKGROUND_PROCESSES parameter in the file to true or false.
Setting the value to true enables the asynchronous background job. If background processes are running, this value prevents OPBackup or OPRestore from starting. True is the default value. false disables the validation check for asynchronous background jobs. OPBackup or OPRestore start even if background processes are running.

The OPBackup utility (Db2)

OPBackup is the IBM OpenPages with Watson utility that backs up the necessary product files on the server where it is run. The OPBackup utility creates a backup file that can be used by the OpenPages restore utility (OPRestore).

When you use the OPBackup utility, the following OpenPages with Watson resources are backed up:

- The OpenPages with Watson application
- The OpenPages with Watson storage folder and its content
- The OpenPages with Watson application environment files

OPBackup does not back up standard tools by default. If you want to include additional files or directories, you must add them to a manifest file before you run the backup. For more information, see “Backing up custom files” on page 549.

Depending on your configuration, if any asynchronous background jobs are detected, the OPBackup job will exit and might display errors (see “Asynchronous background jobs and administrative functions” on page 547).

You can also configure email notification upon completion of an OPBackup. For details, see “[Configuring backup job notification](#)” on page 545.



Attention: If you have global search enabled, global search must be disabled before you run the OPBackup and OPRestore utilities. For more information, see “[Using OPBackup and OPRestore when global search is enabled](#)” on page 520.

Backing up custom files

You can include custom files, such as custom JSPs or other files that are specific to your environment, in backups by using a manifest file. A manifest file is a text file that contains the full path name to any directory or file that needs to be included in the backup.

For example, if you want to back up `openpages-ext.jar`, add its full path to the manifest file:

```
/opt/opuser/IBM/OpenPages/aurora/lib/openpages-ext.jar
```

Before you begin

- You must list all of your custom directories and files in a manifest. If you have any questions about the location of your custom data, contact IBM OpenPages Support.
- In a horizontal clustered environment, you must perform this procedure on each application server in the horizontal cluster.

Procedure

1. Log on to the application server.
2. If you have custom JSPs, do the following steps:
 - a) Create a zip file called `solutions-sosa-files.zip` that contains your custom JSPs and related files.

Tip: You can use a different name, but it must follow the convention `*-sosa-files.zip`. Also, you must add it to the `<OP_HOME>/aurora/bin/op-backup.manifest` file. Only `solutions-sosa-files.zip` is backed up and restored by default.
 - b) Put the `solutions-sosa-files.zip` file in the `<OP_HOME>/applications` directory.
 - When you run OPBackup, the zip file is included in the backup.
 - When you run OPRestore, the zip file is restored to `<OP_HOME>/applications` and is also extracted to `<OP_HOME>/wlp-user/shared/apps/op-apps.ear/taskui.war/`
3. Open the `<OP_HOME>/aurora/bin/op-backup.manifest` file in a text editor.
4. Add custom files or directories, other than JSPs, to the `op_backup.manifest` file.

You can specify directories or individual files. For each file or directory, create a new line and type its full path..
5. Save the manifest file using the current location and name.

Enabling and disabling storage backup

By default, the IBM OpenPages with Watson backup includes the storage folder and its content. You can disable storage backup by setting the `BACKUP_OP_STORAGE` parameter in the `op-backup-restore.env` file.

Procedure

1. Open a command or shell window on the OpenPages with Watson server.
2. Navigate to the `op-backup-restore.env` file in the `bin` directory as follows.

Table 164. Installation locations

Operating system	Installation location
Windows	<OP_HOME>\aurora\bin
Linux	<OP_HOME>/aurora/bin

3. Open the op-backup-restore.env file in a text editor of your choice.
4. Set the value of the BACKUP_OP_STORAGE parameter in the file to one of the following:

Table 165. BACKUP_OP_STORAGE parameter values and their meanings

If the value is set to...	Then...
true	The storage folder and its content are backed up. This is the default value.
false	The storage folder and its content are not backed up.

5. When finished, save the changes to the file and exit the editor.

Configuring OPBackup to use GZIP

If a ZIP backup file grows beyond the 4-GB limit of zip file capacity, you can configure the OPBackup utility to use gzip (GNU zip). After the file is configured, new backup files have a .tar.gz extension. The OPRestore utility detects if a file is in zip or gzip format and processes the file accordingly.

Procedure

1. From a command or shell window, navigate to the op-backup-restore.env file in the bin directory as follows.
 - For Windows, the installation directory is c:\<OP_Home>\aurora\bin
 - For Linux, the installation directory is <OP_HOME>/aurora/bin
2. Open the op-backup-restore.env file in a text editor of your choice.
3. Change the USE_GZIP_COMPRESSION= setting from false to true.

Running the OPBackup command (Db2)

When you use the IBM OpenPages with Watson application backup utility, run the OPBackup command in a command or shell window.

The OPBackup command does the following:

- Stops all OpenPages with Watson services on the local application server before performing any backup operation
- Backs up OpenPages with Watson application and environment files
- Restarts the services on the local application server when the backup activities are complete

Procedure

1. If global search is enabled, disable it:
 - a) Log in to OpenPages as an administrator.
 - b) Click  > **System Configuration** > **Global Search** and click **Disable**.
2. Shut down all non-admin application servers.
3. Open a command or shell window on the OpenPages with Watson admin application server.
4. Navigate to the <OP_HOME>/aurora/bin directory.

5. Run the following backup command:

Linux

```
./OPBackup.sh <path-to-backup-location>
```

Windows

```
OPBackup <path-to-backup-location>
```

Where <path-to-backup-location> is the full path of the directory where the backed up files are located on the OpenPages with Watson application server. If a file path is not specified, the OPBackup command uses the backup location that is specified in the BACKUP_LOCATION parameter of the <OP_HOME>|aurora|bin|op-backup-restore.env file.

Results

The backup process creates a log file in the <backup-directory-name> directory. Each time you run the OPBackup command, a separate log file is generated.

The OpenPages with Watson restore utility on the Db2 database

OPRestore is the IBM OpenPages with Watson restore utility that restores the necessary product files on the server from which it was originally run. The OPRestore utility uses a backup file that is created by the OpenPages backup utility (OPBackup).

Prerequisites

Important: Before you run the OPRestore utility, you must restore the OpenPages database.

The OPRestore tool can be used only with an existing OpenPages database. It cannot be used on a database that does not have an OpenPages schema.

Restoring files

To back up or restore the IBM Db2 databases for IBM OpenPages with Watson, you must use the utilities that are provided with Db2. For more information about the databases in IBM OpenPages with Watson and backing up or restoring them, see “[Database backup and restore for OpenPages \(Db2\)](#)” on page 555.

Note: To refresh a test environment, see “[Refreshing a test environment from backup files](#)” on page 600.

As part of the restoration process, the following OpenPages resources are restored:

- If the OpenPages storage folder was backed up, the storage folder and its content are restored.
For information about enabling and disabling storage folder backup, see “[Enabling and disabling storage backup](#)” on page 549.
- The OpenPages application environment files are restored.

Depending on your configuration, if any asynchronous background jobs are detected, an OPRestore job might exit and possibly display errors. See “[Asynchronous background jobs and administrative functions](#)” on page 547.

Running the OPRestore command (Db2)

You can restore a backup of the OpenPages application by using the OPRestore command. Use these steps if you're using Db2.

Procedure

1. If you enabled the global search component during backup, re-create your search index so that your search results are synchronized.
 - a) Click  > **System Configuration** > **Global Search** and click **Disable**.
 - b) Click **Drop** to drop the search indexes.
 - c) Click **Create** to re-create the search indexes.
2. Stop the IBM Cognos service.
3. Shut down all non-admin application servers.
4. On the admin application server, open a command or shell window.
5. Navigate to the `<OP_HOME>/aurora/bin` directory.
6. Run the following command:

Windows

```
OPRestore <backup-file-name> <path-to-backup-location> app-nodb
```

Linux

```
./OPRestore.sh <backup-file-name> <path-to-backup-location> app-nodb
```

Where:

`<backup-file-name>` is the name of the backup file (without the `.zip` or `.tar.gz` file extension)

Results

The restore process creates a log file in the `<backup-directory-name>` directory. Each time you run the OPRestore command, a separate log file is created.

Using the Cognos Backup utility (Db2)

OPCCBackup is the Cognos utility that backs up the necessary Cognos files. The OPCCBackup utility creates a backup file that can be used by the Cognos restore utility OPCCRestore.

To back up or restore the IBM Db2 databases for IBM OpenPages with Watson, you must use the utilities that are provided with Db2. For more information about the databases in IBM OpenPages with Watson and backing up or restoring them, see “[Database backup and restore for OpenPages \(Db2\)](#)” on page [555](#).

When you use the OPCCBackup utility, the following Cognos resources are backed up.

- Cognos reports
- Branding and environment files

You can configure email notification (with an attached log file) upon the completion of an OPCCBackup. For details, see “[Configuring backup job notification](#)” on page [545](#).

The OpenPages with Watson file storage directory

By default, `OP_DATAPUMP_DIRECTORY` is the name of the directory used for storing Cognos Content Store database backup files. The path to this directory on the database server varies and depends on how it was defined.

If the `OP_DATAPUMP_DIRECTORY` storage directory does not already exist on the database server, you must run the script to create the directory.

Running the OPCCBackup command (Db2)

When you use the Cognos backup utility, you run the OPCCBackup command in a command or shell window.

Procedure

1. From a command or shell window, navigate to the <CC_Home>/tools/bin, where <CC_Home> represents the installation location of the Cognos application.
2. Run the following backup command:

Windows

```
OPCCBackup <path-to-backup-location>
```

Linux

```
OPCCBackup.sh <path-to-backup-location>
```

Where:

<path-to-backup-location> is the full path of the backup directory on the Cognos server. The file path is optional.

Note: If no file path is specified, the OPCCBackup command uses, by default, the backup location that is specified in the BACKUP_LOCATION parameter of the <CC_Home>|tools|bin|op-cc-backup-restore.env file.

Results

The backup process creates a log file in the <backup-directory-name> directory. Each time you run the **OPCCBackup** command, a separate log file is generated.

Cognos backed-up content

The Cognos backup process creates a ZIP file (.zip) in the <backup-directory-name> directory. This ZIP file contains the necessary report and environment files that can be used by the Cognos restore utility (OPCCRestore).

Note:

- If a backup file is very large (4 GB or larger), configure the OPCCBackup utility to use gzip (GNU zip). Gzip produces an archive with an extension of .tar.gz.
- The OPCCBackup utility adds a timestamp to the .zip and log files it creates.

The ZIP file can be used as a parameter to the OPCCRestore command to restore the installation-specific IBM OpenPages with Watson files and the database. Each time the OPCCBackup command is run, a separate ZIP file is created and each data file is identified by a unique name.

Configuring OPCCBackup to use GZIP

If a ZIP backup file grows beyond the 4-GB limit of zip file capacity, you can configure the OPCCBackup utility to use gzip (GNU zip). After the file is configured, new backup files have a .tar.gz extension. The OPCCRestore utility detects if a file is in zip or gzip format and process it accordingly.

Procedure

1. From a command or shell window, navigate to the op-cc-backup-restore.env file in the bin directory as follows, where <CC_Home> represents the installation location of the Cognos application..
 - For Microsoft Windows, the bin directory is <CC_Home>\tools\bin. By default, <CC_Home> is C:\OpenPages\CommandCenter.
 - For Linux, the bin directory is <CC_Home>/tools/bin. By default, <CC_Home> is opt/OpenPages/CommandCenter.

2. Open the `op-cc-backup-restore.env` file in a text editor.
3. Change the `USE_GZIP_COMPRESSION=` setting in the file from `false` to `true`.

Using the Cognos Restore utility

OPCCRestore is the IBM OpenPages with Watson Cognos utility that restores the necessary Cognos files on the server from which it was originally run. The OPCCRestore utility uses a backup file created by the OPCCBackup utility.

Important: Before you run the OPCCRestore utility, you must restore the IBM Db2 reporting database.

To back up or restore the IBM Db2 databases for IBM OpenPages with Watson, you must use the utilities that are provided with Db2. For more information about the databases in IBM OpenPages with Watson and backing up or restoring them, see “[Database backup and restore for OpenPages \(Db2\)](#)” on page [555](#).

As part of the OPCCRestore restoration process, the following Cognos resources are restored:

- Cognos reports
- Branding and environment files

For information about refreshing a test environment, see “[Refreshing a test environment from backup files](#)” on page [600](#).

Running the OPCCRestore command

You can restore backed up Cognos data using the OPCCRestore utility as follows.

Procedure

1. Stop the Cognos service on the administrative server and any non-administrative servers in the cluster. For details, see “[Starting and stopping the Cognos services](#)” on page [717](#).
2. Stop the IBM Cognos Configuration tool, if it is running, on all cluster members.
3. From a command or shell window, navigate to the bin directory as follows:

Where `<CC_HOME>` represents the installation location of the Cognos application.

Table 166. Installation location of the Cognos application

Operating system	Installation location
Windows	<code><CC_HOME>\tools\bin</code> By default, <code><CC_HOME></code> is <code>C:\IBM\OpenPages\CommandCenter</code>
Linux	<code><CC_HOME>/tools/bin</code> By default, <code><CC_HOME></code> is <code>/opt/IBM/OpenPages/CommandCenter</code>

4. On the administrative Cognos server, execute the following command:

Windows

```
OPCCRestore <backup-file-name> <path-to-backup-location>
```

Linux

```
OPCCRestore.sh <backup-file-name> <path-to-backup-location>
```

Where:

`<backup-file-name>` is the name of the backup file (without the `.zip` or `.tar.gz` file extension).

Note: `<path-to-backup-location>` is the full path of the directory where the backed up files are located on the Cognos server. The file path is optional.

Note: If no file path is specified, the OPCCRestore command uses, by default, the backup location specified in the BACKUP_LOCATION parameter of the <CC_Home>|tools|bin|op-cc-backup-restore.env file.

5. Start the Cognos service on the administrative server and on any non-administrative servers in the cluster. For details, see [“Starting and stopping the Cognos services” on page 717](#).

Results

The restore process creates a log file identified by a unique name in the <backup-directory-name> directory. Each time you run the OPCCRestore command, a separate log file is created.

Database backup and restore for OpenPages (Db2)

You must use the utilities that are provided with IBM Db2 to back up and restore Db2 databases for OpenPages.

Note: This task applies to OpenPages with Watson. For information about backing up and restoring databases for IBM OpenPages for IBM Cloud Pak for Data, see [Backing up, restoring, and migrating OpenPages](#).

For information about developing a backup and restore strategy, see the [IBM Db2 documentation](#).

Db2 databases in OpenPages

There are two databases in IBM OpenPages with Watson that require backup:

- The OpenPages with Watson database

This database is the main application database that is created in the Db2 instance with Oracle Compatibility mode enabled.

- The Cognos content store

This database is created in another normal Db2 instance without Oracle Compatibility mode enabled.

OpenPages Db2 database backup

For IBM OpenPages with Watson, to do a complete backup of the IBM OpenPages with Watson and the Cognos databases, you must back up each database from each of their instances. For IBM OpenPages with Watson, The simplest approach is to do an offline backup of your Db2 databases.

1. Make sure that no OpenPages services are running for any long running background processes (such as object reset jobs).
2. Stop the OpenPages services.

For more information, see [Chapter 25, “Starting and stopping servers,” on page 709](#).

3. Open a command or shell window and connect to the Db2 database as the database instance owner.

For Windows users only, you must use the **db2cmd** command in the **Command Prompt** window to initialize the Db2 command line processor (CLP).

4. Start the Db2 instance by using the **db2start** command.
5. Do the offline backup.

For example, on a Linux operating system, to back up a database with the alias name of sample to /opt/db2backup, you can use db2 backup db sample /opt/db2backup. A backup image is created in the specified backup location in the following format:

database_name.backup_type.instance_name.database_partition.catalog_partition_number.backup_date_time.time_image_sequence_number. For example, OPX.0.DB2INST1.NODE0000.CATN0000.20221129.131259.001.

On a Microsoft Windows operating system, to back up a database with the alias name of sample to c:\Db2backup, you can use db2 backup db sample c:\Db2backup. A backup image is created in the specified backup location in the following format:

`database_name.backup_type\instance_name\database_partition\catalog_partition_number\backup_date_time\time_image_sequence_number`. For example, OPX.0\DB2INST1\NODE0000.CATN0000.20221129\131259.01.

For information about backing up your Db2 database, see the [IBM Db2 documentation](#).

6. Start the OpenPages services:

OpenPages Db2 database restore

You can use a Db2 database backup from your production system to restore a Db2 database to a previous state in the same environment.

Use this process as a guide for restoring a OpenPages Db2 database:

1. Stop the OpenPages services:
2. Open a command or shell window and connect to the Db2 database as the database instance owner.

For Windows users only, you must use the **db2cmd** command in the **Command Prompt** window to initialize the Db2 command line processor (CLP).

3. Restore the Db2 database.

For example, on a Linux operating system, to restore a database with the alias name of sample from the backup location /opt/db2backup with a backup timestamp of 20221129131259, you can use db2 restore db sample from /opt/db2backup taken at 20221129131259.

On a Windows operating system, to restore a database with the alias name of sample from the backup location c:\Db2backup with a backup timestamp of 20221129131259, you can use db2 restore db sample from c:\Db2backup taken at 20221129131259.

For information about restoring your Db2 database, see the [IBM Db2 documentation](#).

4. Start the OpenPages services:

Moving a database when you can't use backup and restore

In some cases, it is not possible to move a Db2 database between OpenPages with Watson environments by doing a backup and restore. For example, Db2 does not support using a backup and restore to move a database if the source and target environments are using different operating systems or if the source and target are using different schema names. For more information, see [Backup and restore operations between different operating systems and hardware platforms](#) in the Db2 documentation.

Db2 has several tools and techniques that you can use instead. For more information about how to use these tools with OpenPages, see [Moving Db2 database objects to a new database when a backup and restore cannot be performed](#).

Restoring backed up production data in a new Db2 environment

You can use a IBM Db2 database backup from your production environment to restore data to a Db2 database in a new test or development environment.

The process of restoring data involves the following tasks in this order:

1. Back up your Db2 production databases then restoring these databases to the new environment.

When you create the IBM OpenPages with Watson application database, you must run scripts to enable Oracle compatibility and update configuration data. You run these scripts before you restore the OpenPages with Watson application production database to the new environment. These scripts are not required for the Cognos database.

2. Back up your production application and reporting data files then restore these files to the new environment.
3. Update the storage folder location in the new environment.

For information about refreshing a test environment on an existing test system, see “[Refreshing a test environment from backup files \(Db2\)](#)” on page 558.

Before you begin

Make sure that your new test or development environment meets the following prerequisites:

- OpenPages with Watson is installed in the new test or development environment.
- The operating system user names in the new environment match the operating system user names in your production environment.

Procedure

1. Back up your OpenPages with Watson application production Db2 database.
For more information, see “[OpenPages Db2 database backup](#)” on page 555.
2. Back up your IBM Cognos Controller production Db2 database.
For information about backing up the IBM OpenPages application database, see “[OpenPages Db2 database backup](#)” on page 555.
3. Create the OpenPages with Watson application database instance in the new environment.
For more information about creating a Db2 database, see the IBM Db2 documentation.
4. On the new OpenPages with Watson application database only, run the enable-ora-compatibility script to enable Oracle Compatibility Mode.
In the output, look for the Db2 profile variable, **DB2_COMPATIBILITY_VECTOR**, with the value of ORA. For example, **DB2_COMPATIBILITY_VECTOR=ORA**.

Microsoft Windows

- a. Click **Start > IBM Db2 > DB2COPY1 > Command Window - Administrator**.

Note: If you have multiple instances of Db2 on the server, make sure that you choose the DB2COPY of the OpenPages database instance.

- b. Run the following command: **enable-ora-compatibility.bat**

Linux

Run the following command: **./enable-ora-compatibility.sh**

Note: Db2 compatibility features are enabled at the instance level and cannot be disabled. Keep the selected compatibility level for the life of the OpenPages database. To confirm that Oracle Compatibility Mode is set, type the following command: **db2set -all**

5. On the new IBM OpenPages application database only, update the database manager configuration.
 - a) For Windows users only, type the following command in the **Command Prompt** window to initialize the Db2 command line processor (CLP):


```
db2cmd
```
 - b) In the Db2 CLP, run the `opx-dbm-cfg` script:
 - On Windows, type:
`opx-dbm-cfg.bat`
 - On Linux, type:
`./opx-dbm-cfg.sh`
6. Use the OpenPages with Watson application database backup from your production system to restore the Db2 database to your new environment.

For more information, see “[OpenPages Db2 database restore](#)” on page 556.

7. Create the IBM Cognos Controller database instance in the new environment without the Oracle Compatibility feature.
For more information about creating a Db2 database, see the IBM Db2 documentation.
8. Use the IBM Cognos Controller database backup from your production system to restore the Db2 database to your new environment.
For more information, see "[OpenPages Db2 database restore](#)" on page 556.
9. Use the OpenPages with Watson backup and restore utilities to back up the product files on the production server then restore these files to your new environment.
For more information about using the OpenPages with Watson backup utility, see "[The OPBackup utility \(Db2\)](#)" on page 548.
For more information about using the OpenPages with Watson restore utility, see "[The OpenPages with Watson restore utility on the Db2 database](#)" on page 551.
10. Use the Cognos backup and restore utilities to back up your reporting files on the production server then restore these files to your new environment.
For more information about using the Cognos backup utility, see "[Using the Cognos Backup utility \(Db2\)](#)" on page 552.
For more information about using the Cognos restore utility, see "[Using the Cognos Restore utility](#)" on page 554.
11. Update the OpenPages storage folder location on the new test or development database.
For more information about updating the storage folder location, see "[Update the OpenPages with Watson storage location in the Db2 database](#)" on page 561.

Refreshing a test environment from backup files (Db2)

The best method for refreshing an existing test environment is to have it replicated from the production environment. By using your production environment's backup files, you can update a test environment that closely matches your production environment as of the backup date.

You can use this procedure to refresh a test server by using the backup files from another IBM OpenPages with Watson server.

Prerequisites:

- Make sure that you have access to both the production or "source" and test or "target" servers.
- The operating systems must match between the source and target servers.
- The OpenPages version and patch level must match between the source and target servers.

Prerequisites to refreshing a Db2 test environment

There are some prerequisites to refreshing a test environment.

The following are required:

- The test or "target" server and production or "source" server must have the same installed version of the IBM OpenPages with Watson application - including patches.
- You must have access to the OpenPages with Watson installation files.

Backup of production databases in OpenPages with Watson on the Db2 server

You must use the utilities that are provided with IBM OpenPages with Watson to back up the production databases in the application. The exported IBM Db2 production databases are used later to refresh the OpenPages with Watson application databases on the test or target server.

For more information about the databases in OpenPages with Watson and backing up Db2 databases, see “[Database backup and restore for OpenPages \(Db2\)](#)” on page 555.

Backing up and copying OpenPages with Watson application production files for a Db2 database

The IBM OpenPages with Watson backup utility backs up the application files. The exported data from the production backup file is used later to refresh data on the test or target server.

Procedure

1. Log on to your production OpenPages with Watson server as a user with administrative permissions.
2. Run the OpenPages with Watson backup utility (OPBackup) to back up the application files.
For more information, see “[The OPBackup utility \(Db2\)](#)” on page 548.
3. Copy the backup .zip or .tar.gz file to your test server.

Backup of OpenPages with Watson databases on the test server

You must use the utilities that are provided with IBM Db2 to back up the test or target databases in IBM OpenPages with Watson.

For more information about the databases in OpenPages with Watson and backing up Db2 databases, see “[Database backup and restore for OpenPages \(Db2\)](#)” on page 555.

Backing up OpenPages with Watson application files on your test server

Run the IBM OpenPages with Watson backup utility to back up the application files on your test or target server.

Procedure

1. Log on to your test OpenPages with Watson server as a user with administrative permissions.
2. Run the backup utility (OPBackup) as described in “[The OPBackup utility \(Db2\)](#)” on page 548 to backup the OpenPages with Watson application files.

Running the OPCCBackup command

When you use the Cognos backup utility, you run the OPCCBackup command in a command or shell window.

Procedure

1. From a command or shell window, navigate to the bin directory as follows:

For Microsoft Windows:<CC_Home>\tools\bin By default, <CC_Home> is C:\OpenPages\CommandCenter

For Linux, type <CC_Home>/tools/bin By default, <CC_Home> is /opt/OpenPages/CommandCenter

2. Execute the following backup command:

Windows: OPCCBackup <path-to-backup-location>

Linux: OPCCBackup.sh <path-to-backup-location>

Where:

<path-to-backup-location> is the full path of the directory where the backed up files are located on the Cognos server. The file path is optional.

Note: If no file path is specified, the OPCCBackup command uses, by default, the backup location specified in the BACKUP_LOCATION parameter of the <CC_Home>|tools|bin|op-cc-backup-restore.env file.

Drop the Db2 database for the application on the test system

You must drop the IBM OpenPages with Watson database on the test server. Dropping the IBM Db2 database for IBM OpenPages with Watson on the test system deletes all object data.

The Db2 database includes OpenPages with Watson application data.

Procedure

1. Log on to your IBM OpenPages with Watson test server as a user with administrative permissions.
2. Stop all OpenPages, Cognos, and global search services.
3. Open a command or shell window.
4. For Windows users only, type the following command in the **Command Prompt** window to initialize the Db2 command line processor (CLP):

db2cmd

5. In the Db2 CLP, type the following command to drop the Db2 test database:

db2 drop db <DATABASE_NAME>

Where <DATABASE_NAME> is the name of the test database.

For example, if the name of the test database is op, type db2 drop database op.

Copy and restore the production Db2 database backup file to the test Db2 database server

You must use the utilities that are provided with IBM Db2 to restore the IBM OpenPages with Watson database on the test system.

Before you begin

The operating system user names in the test environment must match the operating system user names in your production environment.

Procedure

1. Copy the OpenPages with Watson database backup file from the Db2 production server to the test database server.
2. Copy the Java UDF class files from the Db2 production server folders to the folders on the test database server.

For example:

- On Windows systems, copy the class files from C:\IBM\SQLLIB\FUNCTION on the production database server to the Db2 database server on the test system.
- On Linux systems, copy the class files from /home/db2inst1/sqllib/function on the production database server to the Db2 database server on the test system.

3. Restore the Db2 database to the test server. For more information, see “[OpenPages Db2 database restore](#)” on page 556.

Update the OpenPages with Watson storage location in the Db2 database

After you restore the openpage-storage files from the production backup, you must update the IBM OpenPages with Watson storage location on the test database.

Procedure

1. Log on to a system as a user with administrator privileges. You can use any system with access to CLPPlus that can connect to the OpenPages database server.
2. Copy all the files under the openpages-storage folder from the production backup .zip file to the openpages-storage location on the test server.

By default, the storage location is <OP_Home>|openpages-storage.

Table 167. Installation location of the OpenPages with Watson application

Operating system	Installation location
Windows	For example, <OP_HOME> C:\IBM\OpenPages
Linux	For example, <OP_HOME> /opt/IBM/OpenPages

3. Open a command or shell window and do the following tasks:
 - a) Go to the INSTALL_SCRIPTS directory in the installation package:
`/OP_<version>_Main/OP_<version>_Configuration/Database/DB2/INSTALL_SCRIPTS`
4. For Windows users only, type the following command in the **Command Prompt** window to initialize the Db2 command line processor (CLP):

db2cmd

5. From the INSTALL_SCRIPTS directory, run the update-storage SQL wrapper script with the following parameters to update the openpages-storage directory location in the database:

- On Windows:

```
clpplus -nw <op_db_user>/<op_db_password>'@<database_host>:<database_port>/<database_name> @sql-wrapper update-storage <log-file><database_host>:<database_port>/<database_name> <op_db_user> '<op_db_password>' <storage-type> <storage-server-name> <host-name> Windows <path-or-UNC-name>
```

- On Linux:

```
clpplus -nw <op_db_user>/<op_db_password> '\@<database_host>:<database_port>/<database_name> @sql-wrapper update-storage <log-file><database_host>:<database_port>/<database_name> <op_db_user> '\<op_db_password>\'<storage-type> <storage-server-name> <host-name> Unix <path-or-UNC-name>
```

Table 168. Update Storage Wrapper Script Parameters

Parameter	Description
<i>op_db_user</i>	The OpenPages user name for accessing the OpenPages database.
<i>op_db_password</i>	The password of the <i>op_db_user</i> user.
<i>database_host</i>	The hostname of the Db2 server that contains the OpenPages database.
<i>database_port</i>	The port number of the Db2 database instance that is installed on the database server. For Db2, the default port is 50000.
<i>database_name</i>	The name of the OpenPages database.
<i>log-file</i>	The name of the log file that the script creates and writes information to.

Table 168. Update Storage Wrapper Script Parameters (continued)

Parameter	Description
<i>storage-type</i>	The type of file storage to be used. Valid values are as follows: <ul style="list-style-type: none"> • LFS (local file system) • UNC (Universal Naming Convention) - for Windows only. Note: After you move from LFS to UNC, you cannot go back to using LFS.
<i>storage-server-name</i>	The name of the storage server.
<i>host-name</i>	The hostname of the machine.
<i>os-type</i>	The type of operating system. Valid values are as follows: <ul style="list-style-type: none"> • Windows • Unix
<i>path-or-UNC name</i>	The file path of the storage location.

Examples

- LFS (Linux) :

```
clppplus -nw openpage/\'password\'@myserver:50000/OPX @sql-wrapper
update-storage log.log myserver:50000/OPX openpage \'password\' LFS server1 server1 Unix /
home/opuser/OP/OpenPages/openpages-storage
```

- LFS (Windows):

```
clppplus -nw openpage/'password'@myserver.ibm.com:50000/OPX @sql-wrapper update-storage
log.log myserver.ibm.com:50000/OPX openpage 'password' LFS server1
server1 Windows C:\openpages-storage
```

- UNC (Windows):

```
clppplus -nw openpage/'password'@myserver.ibm.com:50000/OPX @sql-wrapper update-storage
log.log myserver.ibm.com:50000/OPX openpage 'password' UNC server1
server1 Windows openpages-storage
```

Back up the Cognos database on the Db2 production and test servers

You must use the utilities that are provided with IBM Db2 to back up the IBM Cognos Controller database on both the production and test servers. The exported Db2 production database is used later to refresh the IBM Cognos Controller database on the test or target server.

For more information about the databases in IBM OpenPages and backing up Db2 databases, see [“Database backup and restore for OpenPages \(Db2\)” on page 555](#).

Back up Cognos configuration files on the Db2 production and test servers

You must run the Cognos backup utility to back up Cognos configuration files on both the production and test servers. The Cognos configuration file backup from the production server is used later to refresh Cognos configuration on the test server.

Before you begin

Before you run the Cognos backup utility (OPCCBackup) make sure to verify the following:

- You have access to both the source and target database servers.
- Full permission is granted to the CommandCenter|tools|bin folder on the target Cognos server.

Procedure

1. If necessary, log on to your production Cognos server as a user with administrative permissions.
2. Run the Cognos backup utility (OPCCBackup) to back up the Cognos configuration files on the production server.

For more information, see [“Using the Cognos backup utility” on page 588](#).

Tip: If the mail server for notification email is not set up for running Cognos backups, the output from the OPCCBackup command might end with the following error:

```
BUILD FAILED  
c:\machine3\CommandCenter\tools\bin\op-cc-backup-email-notification.xml:31:  
Problem while sending mime mail:
```

This error can be safely ignored if the step before the error says BUILD SUCCESSFUL.

3. Copy the production Cognos server backup .zip or .tar.gz file to the Cognos backup-restore directory on the test server.
4. Run the Cognos backup utility (OPCCBackup) to back up the Cognos configuration files on your test server.

For more information, see [“Using the Cognos backup utility” on page 588](#).

Modify SSO and LDAP configuration in the test environment

If you are using SSO or LDAP in the test environment, modify the configuration for each if needed. Otherwise, skip this task.

Copy and restore the Cognos production database backup file to the test database server

You must use the utilities that are provided with IBM Db2 to restore the IBM Cognos Controller reporting database on the test system.

Before you begin

The operating system user names in the test environment must match the operating system user names in your production environment.

Procedure

1. Copy the IBM Cognos Controller database backup file from the Db2 production server to the test database server.
2. Restore the Db2 database to the test server. For more information, see [“OpenPages Db2 database restore” on page 556](#).

Drop the Db2 database for Cognos on the Test Server

You must drop the IBM Cognos Controller database on the test server. Dropping the IBM Cognos Controller database on the test system deletes all object data.

Procedure

1. Log on to your IBM OpenPages with Watson test server as a user with administrative permissions.
2. Stop all OpenPages, Cognos, and global search services.
3. Open a command or shell window.
4. For Windows users only, type the following command in the **Command Prompt** window to initialize the Db2 command line processor (CLP):

db2cmd

5. In the Db2 CLP, type the following command to drop the Db2 test database:

```
db2 drop db <DATABASE_NAME>
```

Where <DATABASE_NAME> is the name of the test database.

For example, if the name of the test database is op, type db2 drop database op.

Copy custom deliverables to the test environment

If you are using custom deliverables, you must copy any custom files to the test environment.

Copy custom triggers

You must copy any custom Java actions and triggers that have been deployed on the production server to the test environment. These custom actions and triggers are added to a zip file, openpages-ext.jar, by the OPBackup utility.

If you have any questions about the location of your custom data, contact IBM OpenPages Support.

Procedure

1. If necessary, log on to your test IBM OpenPages with Watson server as a user with administrative permissions.
2. Update the openpages-ext.jar in the test environment as follows:
 - a) From the production backup .zip file, navigate to the openpages-ext.jar in the <OP_Home>|aurora|lib directory.
Where <OP_HOME> represents the installation location of the IBM OpenPages application.

Table 169. Installation location of the OpenPages with Watson application

Operating system	Installation location
Windows	<OP_HOME>\aurora\lib\openpages-ext.jar By default <OP_HOME> is C:\IBM\OpenPages
Linux	<OP_HOME>/aurora/lib/openpages-ext.jar By default <OP_HOME> is /opt/IBM/OpenPages

- b) Copy the openpages-ext.jar from the production backup file into the <OP_Home>|aurora|lib directory on your test machine and overwrite the existing .jar file there.

Copy other custom deliverables to the test environment

If you have other custom deliverables, such as UI helpers and JSP reports, copy these custom deliverables to their respective folders on the test or target machine.

If you have any questions about the location of your custom data, contact IBM OpenPages Support.

Procedure

1. From your application production backup .zip files, extract all custom files such as JAR files, JSP files, JavaScript files, and Image files.
2. Copy these files into their respective folders on the target machine. The target folders should match the folders on the source installation.

Starting OpenPages with Watson in the test environment

When finished, start IBM OpenPages with Watson services on the servers in your test environment.

For details, see [Chapter 25, “Starting and stopping servers,” on page 709](#).

Updating the OPSystem password

If the OPSystem password is different in the source (production) and target (test) environments or if you changed the default OPSystem password, update the OPSystem password in the test environment.

For more information, see [“Changing the OPSystem password” on page 637](#).

Update Db2 database connection references for Cognos

You must update the database connection references for the server on the IBM Cognos Analytics.

Procedure

1. From a browser, log on to IBM Cognos Analytics as a user with administrative privileges, for example, OpenPagesAdministrator.

By default, the URL is `http://<hostname>/ibmcognos/bi`
Where <hostname> is the name of the Cognos server.
2. Click **Manage > Administration Console** to launch the **IBM Cognos Administration** page.
3. On the **Configuration** tab, click **Data Source Connections** (if not already selected).
4. On the **Directory > Cognos** page, click the link for the **OpenPages DataSource**.
5. On the **Directory > Cognos > OpenPages DataSource** page, do the following:
 - a) Under the **Actions** column, click the **Set properties - OpenPages DataSource** icon .
 - b) On the **Set properties - OpenPages DataSource** page, click the **Connection** tab.
6. On the **Connection** tab, next to the **Connection String** box, click the pencil icon to edit the field.
7. On the **CLI** tab, in the **DB2 database name** box, change the Db2 database name to the Catalog Database Name of the OpenPages with Watson database on the target environment.
8. On the **JDBC** tab, in the **Server name**, **Port number**, and **Database name** boxes, change the values to valid values for the OpenPages with Watson database on the target environment.

Update URL host pointers for Cognos reports

Modify the URL host pointer settings and then propagate these changes to the reporting schema on the application server (does not require services to be restarted).

For more information, see [“Updating URL host pointers for reports” on page 633](#).

Update the global search settings

After you import data from a production environment (the source environment) into a test or development environment (the target environment), you need to update the global search settings.

About this task

When you import data from the source environment, the settings for the search server are imported. You need to update the target environment so that it uses the search server in your target environment.

Procedure

1. Log in to the OpenPages application in the target environment as a user with administrative privileges.
2. Click  > **System Configuration** > **Global Search** and click **Disable**.
3. Stop the global search services.
For more information, see “[Start or stop the global search services](#)” on page 712.
4. Update the global search settings.
 - a) Click **System Configuration** > **Settings** > **Applications** > **Common** > **Configuration** > **Show Hidden Settings** and set the value to **true**.
 - b) Click **System Configuration** > **Settings** > **Platform** > **Search** > **Admin** and update the **Search Server Administration URL** with the URL of the search server in your target environment.
 - c) Click **System Configuration** > **Settings** > **Platform** > **Search** > **Index** and update the **Search Server URL** with the URL of the search server in your target environment.
 - d) Click **System Configuration** > **Settings** > **Platform** > **Search** > **Request** and update the **Search Server URL** with the URL of the search server in your target environment.
5. Copy the `<SEARCH_HOME>/openpages-solr-index` directory to the search server in the target environment.
The `<SEARCH_HOME>/openpages-solr-index` contains the global search index.
6. Start the global search services.
For more information, see “[Start or stop the global search services](#)” on page 712.
7. Click  > **System Configuration** > **Global Search** and click **Enable**.

Results

Global search is enabled in the target environment.

Utilities for filtering on long string field content in a Db2 database

You can filter based on the content of long string fields if the IBM Db2 Text Search feature is enabled. This feature is also known as full text searching.

The Db2 Text Search feature is installed and configured during the IBM OpenPages with Watson installation process. For more information, see the *IBM OpenPages with Watson Installation and Deployment Guide*



Warning: Do not include long string fields that are encrypted using field level encryption in the search criteria because they can return unexpected results.

Long string fields allow users to enter values over 4 KB in length. For information about setting up long text fields, see “[Long String data type](#)” on page 157.

You can do the following tasks to manage full text searching:

- “[Create a long string index in a Db2 database](#)” on page 568
- “[Change the scheduled job that synchronizes the long string index in the database \(Db2\)](#)” on page 570
- “[Drop a long string index](#)” on page 571
- “[Enable Db2 text search](#)” on page 567

For information about how to disable Db2 text search, see [Disabling a database for Db2 Text Search](#).

To apply filters with long string fields, you must change the **Platform** > **Database** > **Text Indexes** setting to **true**.

If the value is set to true, filtering is enabled on long string fields. The default value is false.

For details on working with settings, see [Chapter 20, “Viewing the Configuration and Settings page,”](#) on page 473.

Enable Db2 text search

Enable the IBM Db2 Text Search feature to filter based on the contents of fields with long string data types.

Procedure

1. Log on to a system as a user with Administrator privileges. You can use any system with access to CLPPlus that can connect to the IBM OpenPages with Watson database server.

Note: For SQL tool information, see the *Database tool information* topic at “[Introduction](#)” on page [xxi](#).

2. Open a command or shell window, navigate to the text-indexing directory as follows:

Windows

```
<OP_HOME>\aurora\bin\full-text-index
```

Linux

```
<OP_HOME>/aurora/bin/full-text-index
```

3. Run the following SQL script:

```
clppplus -nw @sql-wrapper CustomIndexing_Step1_AddTextIndexing_to_DB.sql <LOG_FILE_NAME>
<DB2_SERVER_NAME>:<DB2_PORT_NUMBER>/<DATABASE_NAME> <DB2_INSTANCE_OWNER_NAME>
<DB2_INSTANCE_OWNER_PASSWORD> <OP_DB_USER>
```

Table 170. Enable Db2 Text Search required script parameters

Required Parameter	Description
<LOG_FILE_NAME>	Name of the log file.
<DB2_SERVER_NAME>	Name of the Db2 server.
<DB2_PORT_NUMBER>	Port number of the Db2 database service
<DATABASE_NAME>	Name of the OpenPages database.
<DB2_INSTANCE_OWNER_NAME>	Database instance owner account. Usually db2admin user.
<DB2_INSTANCE_OWNER_PASSWORD>	Password for instance owner account. If the password contains special characters, surround the password in quotation marks: <ul style="list-style-type: none">• Windows: "password"• Linux: 'password'
<OP_DB_USER>	OpenPages user name for accessing the OpenPages database.

For example:

- Windows:

```
clppplus -nw @sql-wrapper CustomIndexing_Step1_AddTextIndexing_to_DB.sql
CustomIndexing_Step1_AddTextIndexing_to_DB.log server1:50000/opx db2admin
"password" OPENPAGES
```

- Linux:

```
clppplus -nw @sql-wrapper CustomIndexing_Step1_AddTextIndexing_to_DB.sql
CustomIndexing_Step1_AddTextIndexing_to_DB.log server1:50000/opx db2admin
```

```
'password' OPENPAGES
```

Results

The database is now enabled for indexing. Use “[Create a long string index in a Db2 database](#)” on page 568 script to create the index.

Create a long string index in a Db2 database

Create a long string text index to support filtering based on the contents of fields with long string data types. Scripts are provided for Microsoft Windows and Linux.

Important: In Linux operating systems, when using asterisks (*) as parameter values in long string search scripts, the asterisks must be properly escaped with a double quotation mark, single quotation mark combination: "“*”".

Before you begin

Complete the following tasks:

- [“Enable Db2 text search” on page 567.](#)
- Ensure that the Db2 text search server information is set up.

For more information, see [Updating Db2 Text Search server information](#).

Procedure

1. Log on to a system as a user with Administrator privileges. You can use any system with access to CLPPlus that can connect to the IBM OpenPages with Watson database server.

Note: For SQL tool information, see the *Database tool information* topic at “[Introduction](#)” on page xxi.

2. Open a command or shell window, navigate to the text indexing directory as follows.

The following table identifies the installation location of the application on the Microsoft Windows and Linux operating systems.

Table 171. Installation location of the full-text-index directory

Operating system	Installation location
Windows	<OP_HOME>\aurora\bin\full-text-index
Linux	<OP_HOME>/aurora/bin/full-text-index

3. Run the following script:

```
clppplus -nw @sql-wrapper CustomIndexing_Step2_IndexCreate.sql  
<LOG_FILE_NAME> <DB2_SERVER_NAME>:<DB2_PORT_NUMBER>/<DATABASE_NAME>  
<OP_DB_USER> <OP_DB_PASSWORD> <UPDATE_FREQUENCE_WEEKDAY>  
<UPDATE_FREQUENCE_HOUR> <UPDATE_FREQUENCE_MINUTE> <MINIMUM_UPDATES>
```

Table 172. Create Db2 long string index required script parameters

Required Parameter	Description
<LOG_FILE_NAME>	Name of the log file.
<DB2_SERVER_NAME>	Name of the Db2 server.
<DB2_PORT_NUMBER>	Port number of the Db2 database service
<DATABASE_NAME>	OpenPages database name.

Table 172. Create Db2 long string index required script parameters (continued)

Required Parameter	Description
<OP_DB_USER>	OpenPages user name for accessing the OpenPages database.
<OP_DB_PASSWORD>	OpenPages password for accessing the OpenPages database. If the password contains special characters, surround the password in quotation marks: <ul style="list-style-type: none"> • Windows: "password" • Linux: 'password'
<UPDATE_FREQUENCE_WEEKDAY>	Weekday update frequency. Accepted values are between 0 and 6; multiple values can be separated with a comma. For all weekdays use * (asterisk).
<UPDATE_FREQUENCE_HOUR>	Hourly update frequency. Accepted values are between 0 and 23; multiple values can be separated with a comma. For all hours use * (asterisk).
<UPDATE_FREQUENCE_MINUTE>	Minute update frequency. Accepted values are between 0 and 59, multiple values can be separated with a comma. Typically, values are specified as top of the hour (0), or in multiples of 5 minute increments after the hour, for example, 0, 5, 10, 15, 20, 25, 30, 35, 40, 45, 50 or 55.
<MINIMUM_UPDATES>	Minimum number of updates in the base table before a scheduled index updates is run.

The following example shows a Windows script:

```
clpplus -nw @sql-wrapper CustomIndexing_Step2_IndexCreate.sql
CustomIndexing_Step2_IndexCreate.log server1:50000/opx opuser
"password" "*" "*" "0,5,10,15,20,25,30,35,40,45,50,55" 1
```

The following example shows the same script on Linux:

```
clpplus -nw @sql-wrapper CustomIndexing_Step2_IndexCreate.sql
CustomIndexing_Step2_IndexCreate.log server1:50000/opx opuser
'password' ''*'' ''*'' "0,5,10,15,20,25,30,35,40,45,50,55" 1
```

These examples create an index with updates that start every 5 minutes of every hour of every weekday if there is a minimum of one update to the PROPERTYVALS_CLOB table.

Results

An index is created for long string fields.

Change the scheduled job that synchronizes the long string index in the database (Db2)

You can change the scheduled job that synchronizes the long string index. Scripts are provided for Windows and Linux.

When you install IBM OpenPages with Watson with Db2, you set up Db2 Text Search and create a job to synchronize the indexes. Do this task to refresh the indexes and the scheduled job.

Procedure

1. Log on to a system as a user with Administrator privileges. You can use any system with access to CLPPlus that can connect to the IBM OpenPages with Watson database server.

Note: For SQL tool information, see the *Database tool information* topic at [“Introduction” on page xxi](#).

2. Run the following script:

```
clppplus -nw @sql-wrapper CustomIndexing_Step3_IndexRefresh.sql <LOG_FILE_NAME>
<DB2_SERVER_NAME>:<DB2_PORT_NUMBER>/<DATABASE_NAME> <OP_DB_USER> <OP_DB_PASSWORD>
<UPDATE_FREQUENCE_WEEKDAY> <UPDATE_FREQUENCE_HOUR> <UPDATE_FREQUENCE_MINUTE>
<MINIMUM_UPDATES>
```

Table 173. Refresh Db2 index required script parameters

Required Parameter	Description
<LOG_FILE_NAME>	Name of the log file.
<DB2_SERVER_NAME>	Name of the Db2 server.
<DB2_PORT_NUMBER>	Port number of the Db2 database service
<DATABASE_NAME>	OpenPages database name.
<OP_DB_USER>	OpenPages user name for accessing the OpenPages database.
<OP_DB_PASSWORD>	OpenPages password for accessing the OpenPages database. If the password contains special characters, surround the password in quotation marks: <ul style="list-style-type: none">Windows: "password"Linux: 'password'
<UPDATE_FREQUENCE_WEEKDAY>	Weekday update frequency. Accepted values are 0 - 6; multiple values can be separated with a comma. For all weekdays, use * (asterisk).
<UPDATE_FREQUENCE_HOUR>	Hourly update frequency. Accepted values are 0 - 23; multiple values can be separated with a comma. For all hours, use * (asterisk).

Table 173. Refresh Db2 index required script parameters (continued)

Required Parameter	Description
<UPDATE_FREQUENCE_MINUTE>	Minute update frequency. Accepted values are 0 - 59, multiple values can be separated with a comma. Typically, values are specified as top of the hour (0), or in multiples of 5-minute increments after the hour, for example, 0, 5, 10, 15, 20, 25, 30, 35, 40, 45, 50 or 55.
<MINIMUM_UPDATES>	Minimum number of updates in the base table before a scheduled index updates is run.

The following example shows a Windows script:

```
clppplus -nw @sql-wrapper CustomIndexing_Step3_IndexRefresh.sql
CustomIndexing_Step3_IndexRefresh.log server1:50000/opx OPENPAGE "password"
"*" "*" "0,5,10,15,20,25,30,35,40,45,50,55" 1
```

The following example shows the same script on Linux:

```
clppplus -nw @sql-wrapper CustomIndexing_Step3_IndexRefresh.sql
CustomIndexing_Step3_IndexRefresh.log server1:50000/opx OPENPAGE 'password'
"'*' '*' "0,5,10,15,20,25,30,35,40,45,50,55" 1
```

These examples schedule index synchronization to start every 5 minutes of every hour of every weekday if there is a minimum of one update to the PROPERTYVALS_CLOB table.

Results

Index synchronization jobs run at the interval specified.

Note: Changes to long string fields are not available for filtering until the next scheduled index job runs.

Drop a long string index

Remove the long string index. An index must be dropped before it can be re-created. Scripts are provided for Windows and Linux.

For more information about working with long string indexes, see [Text search index maintenance](#).

Procedure

1. Log on to a system as a user with Administrator privileges. You can use any system with access to CLPPlus that can connect to the IBM OpenPages with Watson database server.

Note: For SQL tool information, see the *Database tool information* topic at [“Introduction” on page xxi](#).

2. Open a command or shell window, and navigate to the text-indexing directory as follows:

Windows

```
<OP_HOME>\aurora\bin\full-text-index
```

Linux

```
<OP_HOME>/aurora/bin/full-text-index
```

3. Run the following SQL script:

```
clppplus -nw @sql-wrapper CustomIndexing_Step5_IndexDrop.sql <LOG_FILE_NAME>
<DB2_SERVER_NAME>:<DB2_PORT_NUMBER>/<DATABASE_NAME> <OP_DB_USER> <OP_DB_PASSWORD>
<FORCE_DROP_INDEX>
```

Table 174. Enable Db2 drop index required script parameters

Parameter	Description
<LOG_FILE_NAME>	Name of the log file.
<DB2_SERVER_NAME>	Name of the Db2 server.
<DB2_PORT_NUMBER>	Port number of the Db2 database service
<DATABASE_NAME>	Name of the OpenPages database instance.
<OP_DB_USER>	OpenPages user name for accessing the OpenPages database.
<OP_DB_PASSWORD>	OpenPages password for accessing the OpenPages database. If the password contains special characters, surround the password in quotation marks: <ul style="list-style-type: none"> • Windows: "password" • Linux: 'password'
<FORCE_DROP_INDEX>	Drops the index without regard to the status of any associated scheduled task. Values are Y (for Yes) or N (for No)

For example:

- Windows:

```
clpplus -nw @sql-wrapper CustomIndexing_Step5_IndexDrop.sql
CustomIndexing_Step5_IndexDrop.log localhost:50000/OPX OPENPAGE
"password" Y
```

- Linux:

```
clpplus -nw @sql-wrapper CustomIndexing_Step5_IndexDrop.sql
CustomIndexing_Step5_IndexDrop.log localhost:50000/OPX OPENPAGE
'password' Y
```

Results

You must re-create the index before you filter on the content of long string fields again. For details on creating a long string index, see [“Create a long string index in a Db2 database” on page 568](#).

Entity Move/Rename utility

The IBM OpenPages with Watson Entity Move/Rename utility allows batch processing of multiple Business Entities for overnight or weekend execution without running the risk of operations that time out. You can run the utility interactively or as a scheduled job.

Using the Entity Move/Rename utility, you can do the following:

- Rename a Business Entity hierarchy
- Simultaneously rename and move a Business Entity hierarchy

A single batch job can contain multiple independent operations, multiple dependent operations, or any combination thereof.

Each operation provides transactional consistency. If an operation fails, all the pending changes for this operation are rolled back. If an operation succeeds, all the changes are persisted.

Each rename, move, or combined operation runs in its own transactional context. So, failure in one operation does not result in the failure of the entire batch job.



CAUTION: Before running the utility, you must stop all application services to avoid data or security errors.

Entity Move/Rename utility prerequisites

Before you use the IBM OpenPages with Watson Entity Move/Rename utility, consider these prerequisites.

- A physical computer or VM that meets the OpenPages with Watson installation requirements. For detailed specifications, see the *IBM OpenPages with Watson Installation and Deployment Guide*.
- An application that produces either CSV (comma-separated value) files or Unicode tab delimited files. This application can be installed on any computer in your environment and is used to prepare the input data for the utility.
- User name and password for the Oracle or IBM Db2 account that owns the OpenPages application database schema (for example, OPENPAGES).

Configuring the Entity Move/Rename utility for a Db2 database

You must configure parameters in the OpenPages with Watson Entity Move/Rename utility before you use it in an IBM Db2 database environment.

Procedure

1. Go to the Entity Move/Rename utility installation location as follows:
`OP_Home|aurora|bin|batch_entity_move_rename_relative`
2. Open the `batch-entity-move-rename.ini` configuration file for editing.
3. Specify appropriate values for the following parameters for a Db2 database environment:

Table 175. Parameters for a Db2 database in the batch-entity-move-rename.ini file:

Parameter Name	Description
server_name	Db2 database server.
port_number	Db2 service port number.
db_Name	OpenPages database name on Db2.
user_name	OpenPages database user name.
password	OpenPages database user password.
data_format	Format of the input file to the utility. Example: csv or unicode-text.
input_file	Name of the input file (including extension). Example: 'Sample-batch-entity-move-rename.txt'

*Table 175. Parameters for a Db2 database in the batch-entity-move-rename.ini file:
(continued)*

Parameter Name	Description
code_page	<p>Code page that is used in the Db2 database.</p> <p>If the data_format parameter is set to the following value:</p> <ul style="list-style-type: none"> • csv saved from Microsoft Excel, it is encoded in ANSI, then the code page must be set to 1252. • unicode-text and encoded in UTF-8 without BOM, then the code page must be set to 1208.
skip_rows	<p>The number of rows in the input files to skip on load.</p> <p>Example</p> <p>If the first row of the file:</p> <ul style="list-style-type: none"> • Contains a list of column names, set the value to '1'. • Does not contain a list of column names, set this value to '0'.

4. Save and close the batch-entity-move-rename.ini configuration file.
5. Prepare the input file. See “[Prepare the input file for the Entity Move/Rename utility](#)” on page 574.

Prepare the input file for the Entity Move/Rename utility

The input file for the Entity Move/Rename utility can be in CSV or Unicode tab delimited format. You can use any editor to create the input files. Included in the utility installation folder is a sample Unicode text file (.txt format).

Important: On Linux, the text input file must be saved or converted to be encoded in UCS-2 Little Endian and have Linux end of line (LF) characters.

Tip: If you are using Microsoft Excel, you must save the spreadsheet as a CSV or tab delimited file.

The input file must have the following five columns of data:

Table 176. Columns in the input file

Column Name	Description	Sample Value
Source entity location	The entity on which the operation is run.	/The Bank/USA/North East/Providence
Target entity location	<p>The new parent entity for "move" and "move and rename" operations only.</p> <p>Note:</p> <ul style="list-style-type: none"> • For Oracle "rename" operations only (no move), the value must be "-" (dash). • For Db2 "rename" operations only (no move), the value must be blank. 	<p>For "move" and "move and rename" operations:</p> <p>/Worldwide/ Americas/USA/NE</p>
Run as user	Application user name, whose identity is used to run the operation.	OpenPagesAdministrator

Table 176. Columns in the input file (continued)

Column Name	Description	Sample Value
New entity name	<p>The new name after the operation for "rename" and "move and rename" operations only.</p> <p>Note:</p> <ul style="list-style-type: none"> For Oracle "move" operations only (no rename), the value must be "-" (dash). For Db2 "move" operations only (no rename), the value must be blank. 	For "rename" and "move and rename" operations: Boston
Execution order	<p>Establishes the operation execution order as follows:</p> <ul style="list-style-type: none"> Operations that specify the execution order are run before operations that do not. Operations that have a numeric value in the execution order column are run in regular ascending ordering. <p>If set, the value must be a valid number; Otherwise, leave the field blank.</p>	1

The following is a short description of the data in the sample .txt file that is included in the utility directory.

- The first line illustrates moving entity /The Bank/USA/North East/Providence to new location /Worldwide/Americas/USA/NE. Operation is to be run as the user SOXAdministrator. This operation is run first in the batch.
- The second line illustrates in place rename of the entity /Worldwide/Americas/USA/NE Providence. Entity name changes to Boston. Target location does not apply and is set to "-". This entry has a dependency on the previous move operation and has higher number in the execution order column. Also, it references to the new entity location that will be in effect after the first operation completes.
- If the first operation fails for any reason, this operation fails as well and the entity location would be incorrect.
- The third line illustrates simultaneous move of the entity /The Bank/USA/Midwest/Chicago to new location /Worldwide/Americas/USA/MW and rename to Detroit. This operation has no dependencies and will be run after the first two complete.

If you have an Oracle database with the 32-bit SQL*Loader utility in a Linux environment, see the topic: [“Avoid error 0509-036 when you use the 32-bit Oracle SQL*Loader”](#) on page 625. Otherwise, run the IBM OpenPages with Watson Entity Move/Rename utility.

Running the Entity Move/Rename utility interactively for a Db2 database

Use the following steps to run the IBM OpenPages with Watson Move/Rename utility interactively in an IBM Db2 database environment.

Before you begin, make sure that you prepared the input file. See [“Prepare the input file for the Entity Move/Rename utility”](#) on page 574 for instructions.

Procedure

- Move the input file into the utility installation directory, which is at:

```
OP_Home|aurora|bin|batch_entity_move_rename_relative
```

2. Validate that the **input_file** parameter in the batch-entity-move-rename.ini configuration file is correctly set to the input file name. For more information, see “[Configuring the Entity Move/Rename utility for a Db2 database](#)” on page 573.
3. For Windows operating systems only: Start the Db2 command line processor first by opening a command window and entering the **db2cmd** command.
4. From the location where the utility is installed, run the batch command file and review the output on the screen.

Windows

```
batch-entity-move-rename.cmd
```

Linux

```
batch-entity-move-rename.sh
```

5. Upon completion, review the following log files for any errors:

- batch-entity-move-rename-load.log
- batch-entity-move-rename-proc.log

If any errors are reported and you are unable to fix them, contact IBM OpenPages Support. Make sure you supply a copy of the screen that contains the error messages and all the log files that are generated by the tool.

Running the Entity Move/Rename utility as a scheduled task

You can set up a scheduled task to run the IBM OpenPages with Watson Entity Move/Rename utility.

Depending on your environment, you can run the batch-entity-move-rename batch command file by using any scheduling application. For example, in Windows, you might use the built-in Windows scheduler. In Linux, you might set up a **cron** job.

Important: If you are using a Db2 database in a Windows environment, you must run the batch command file within the **Db2 Command Line Processor**.

If the job fails, the batch command returns a non-zero exit code. You can redirect the console output to a log file. For example, in Windows:

```
batch-entity-move-rename.cmd >> batch-entity-move-rename.log
```

The following files are overwritten on each run:

- batch-entity-move-rename-load.log
- batch-entity-move-rename-proc.log

These files can be saved, either manually or through a script, if log archives are needed.

Impact of the Entity Move/Rename utility on the OpenPages application

The Entity Move/Rename utility works directly against the IBM OpenPages with Watson database repository. As a result, the Java based OpenPages application is unaware of the changes made to the entity hierarchy and folder structure.

As a result, internal application caches might become out of sync with the data in the repository and lead to discrepancies in the application user interface.

It is required that after you run the tool you restart application services, or run the tool when application services are stopped.

Also, ensure that the **OPBackup** command is not running during execution, and that all batch rename and move operations are completed before you run a backup.

Chapter 23. Using IBM OpenPages with Watson utilities with Oracle databases

You can use these utilities with your Oracle database for backing up and restoring OpenPages with Watson and Cognos files and databases, and setting up a test environment.

Oracle databases and the backup and restore utilities

The backup and restore utilities are installed during the IBM OpenPages with Watson installation.

Use these utilities to back up and restore the OpenPages with Watson environment:

- OpenPages with Watson backup (OPBackup) and restore (OPRestore) are used to backup and restore the OpenPages with Watson application and database
- Cognos backup (OPCCBackup) and restore (OPCCRestore) are used to backup and restore OpenPages with Watson Cognos files and the content store.
- Users can choose to execute a live OPBackup. When running live OPBackup, OpenPages with Watson services are not restarted on the application server, allowing for maximum uptime of the application. By default, the services will be restarted.

Prerequisite: Oracle client software

To use the backup and restore utilities that are included with IBM OpenPages with Watson, the Oracle client software must be installed on both the OpenPages with Watson application server and OpenPages with Watson Cognos server machines.

Note: For the currently supported versions of the Oracle client software, see the [Supported Environments](#) web page or the *IBM OpenPages with Watson Installation and Deployment Guide*.

Oracle Data Pump

Oracle Data Pump provides a server-side infrastructure for very high-speed loading and unloading of data and metadata to and from the database.

Oracle Data Pump is used by the IBM OpenPages with Watson application and Cognos backup and restore utilities and was automatically configured during the OpenPages with Watson installation or upgrade process. If necessary, you can modify Oracle Data Pump settings.

Important:

- The Oracle Data Pump utility creates database backups on the database server. To ensure the database backups are available in the event of a server failure, make sure to copy these backup (dump) files to a different server or external device (such as a tape drive) after the OPBackup or OPCCBackup tool has completed.
- Before you use the Cognos backup utility for the first time, you must configure the Oracle Data Pump datapump directory. You do this by running an SQL script. For details, see “[Configuring or updating the Oracle Data Pump directory](#)” on page 589.

If you change the name or location of the datapump directory, you can also use this script to update the configuration information.

- Oracle Data Pump commands IMPDP and EXPDP should be used because the IMP and EXP commands are not supported.

Configuring backup job notification

You can configure email notification when you complete an IBM OpenPages with Watson application backup or Cognos backup job.

About this task

Log files for email notification are stored in the logs folder in the following locations. A timestamp is included in the log file names.

- For OPBackup (OpenPages with Watson application backup):

```
<OP_Home>|aurora|bin|logs
```

- For OPCCBackup (Cognos backup):

```
<CC_Home>|tools|bin|logs
```

Make sure to set rules in your email client to never send emails from the OpenPages with Watson application server to the Spam or Junk mail folders.

Procedure

1. Open a command or shell window and do one of the following.
 - a) For an OPBackup (OpenPages with Watson application backup), navigate to the op-backup-restore.env file in the <OP_HOME>/aurora/bin directory.
 - b) For a OPCCBackup (Cognos backup), navigate to the op-cc-backup-restore.env file in the bin directory where <cc_home> represents the installation of Cognos.
 - For Microsoft Windows, the back up path is OPBackup <path-to-back-up-location>
 - For Linux, the back up path is OpBackup.sh <path-to-back-up-location>where <path-to-backup-location> is the full path of the directory where the backed up files are located on the application server. If a file path is not specified, the OPBackup command uses, by default, the backup location specified in the BACKUP_LOCATION parameter of the <OP_Home>|aurora|bin|op-backup-restore.env file.
2. Open the selected .env file in a text editor.
3. Specify a value after the equal sign (=) for the parameters described in the following table and save the .env file.

Table 177. Backup email parameters

Parameter name	Description
BACKUP_EMAIL_NOTIFICATION_SERVER=	The hostname of the outgoing mail server.
BACKUP_EMAIL_NOTIFICATION_TO_EMAIL_ID=	The name of recipients that will receive the email notification. Separate email addresses with a comma (,). Note: Do not type a comma after the last email address. Example emailid1@yourdomain.com,emailid2@yourdomain.com

Table 177. Backup email parameters (continued)

Parameter name	Description
BACKUP_EMAIL_NOTIFICATION _FROM_EMAIL_ID=	The name that will appear as the sender of the notification email in the From: field of the email. The email address is also used as the personal name.
BACKUP_EMAIL_NOTIFICATION _SUCCESS_MSG_ FILE=BACKUP_SUCCESS_MSG.txt	The BACKUP_SUCCESS_MSG.txt file is the default file containing the message text that will be used if the OPBackup.cmd completes successfully. You can modify the message text in the BACKUP_SUCCESS_MSG.txt file. The first line of the file is used as the email's subject.
BACKUP_EMAIL_NOTIFICATION _FAIL_MSG_FILE= BACKUP_FAIL_MSG.txt	The BACKUP_FAIL_MSG.txt file is the default file that contains the message text that is used if the OPBackup.cmd fails with errors. You can modify the message text in the BACKUP_FAIL_MSG.txt file as wanted. The first line of the file is used as the email's subject.

Asynchronous background jobs and administrative functions

IBM OpenPages with Watson supports asynchronous execution of processes in the background.

The most common examples of these types jobs are FastMap web-based data import jobs, object resets, and reporting schema generation.

For example, after a user submits a data import file, that file is queued for loading and the import process occurs in the background. Because it is important for asynchronous background jobs to run to completion, certain administrative operations are suspended until all background jobs complete.

By default, the following administrative functions will not start until background jobs are complete:

- OPBackup command
- OPRestore command
- System Administrative Mode (SAM)

Note: To disable the default setting that checks for background jobs before you start **OPBackup** or **OPRestore**, see “[Enabling and disabling asynchronous background processes checking](#)” on page 548.

If asynchronous processes are found, error messages are written to the OPBACKUP restore log. The .log file name has the format op_backup_<yyyy_mm_dd_hh_mm_ss>.log. For example:

- On Windows: C:\OpenPages\openpages-backup-restore\op_backup_2019_07_26_09_35_42.log
- On Linux: /opt/OpenPages/openpages-backup-restore/op_backup_2019_07_26_09_35_42.log

Example

The following samples show the error log message that occurred when an OPBackup command was initiated while the reporting schema was still being generated.

IBM Db2

- For IBM Db2 environments, a sample error log message might look similar to this text:
 - can-proceed:

```
[exec] ERROR near line 26:  
[exec] SQL0438N Application raised error or warning with diagnostic  
[exec] text: "There are existing processes running. Please let them  
[exec] finish or termi".
```
 - can-proceed:

```
[exec] ERROR near line 26:  
[exec] SQL0438N Application raised error or warning with diagnostic  
[exec] text: "There are existing object reset operations running.  
[exec] Please let them finish or termi".
```

Oracle database

For Oracle environments, a sample error log message might look similar to this text:

- can-proceed:

```
[exec] declare  
[exec] *  
[exec] ERROR at line 1:  
[exec] ORA-20001: There are existing processes running.  
[exec] Please let them finish or terminate them before proceeding.  
[exec] ORA-06512: at line 7  
[exec]
```
- can-proceed:

```
[exec] declare  
[exec] *  
[exec] ERROR at line 1:  
[exec] ORA-20001: There are existing object reset operations running.  
[exec] Please let them finish or terminate them before proceeding.  
[exec] ORA-06512: at line 7  
[exec]
```

Enabling and disabling asynchronous background processes checking

By default, IBM OpenPages with Watson does not allow a backup (OPBackup) or restore (OPRestore) operation to start until all asynchronous background jobs are complete.

It is best to run all jobs to completion before you start a backup or restore operation. However, this check can be enabled or disabled as follows.

Procedure

1. Open a command or shell window on the OpenPages with Watson server.
2. Navigate to the op-backup-restore.env file in the <OP_Home>/aurora/bin directory.
3. Open the op-backup-restore.env file in a text editor.
4. Set the CHECK_BACKGROUND_PROCESSES parameter in the file to true or false.
Setting the value to true enables the asynchronous background job. If background processes are running, this value prevents OPBackup or OPRestore from starting. True is the default value. false disables the validation check for asynchronous background jobs. OPBackup or OPRestore start even if background processes are running.

Encrypting database passwords in the backup-restore utility environment files

Passwords that are used by the IBM OpenPages with Watson, and Cognos database user accounts within the backup-restore environment files are encrypted, by default, during installation.

If you change the value of the password parameters within the following environment files, the value is in plain text until it is encrypted.

- op-backup-restore.env database password parameters (the file is stored on the application server):
 - DB_SYSTEM_PWD=
 - DB_SYS_PWD=
 - DB_OP_PWD=
- op-cc-backup-restore.env database password parameters (the file is stored on the reporting server):
 - DB_CC_PWD=

For security purposes, encrypt the changed passwords by completing the following procedure.

Important: In a horizontal clustered environment, you must complete this procedure on each application server or reporting server in the horizontal cluster.

Procedure

1. Open a command or shell window on the OpenPages with Watson server.
2. Go to the <OP_HOME>/aurora/bin directory.
3. To encrypt changed database password parameters in the op-backup-restore.env environment file, run the following command:
 - On Windows operating systems: OPBackup.cmd secure
 - On Linux operating systems: ./OPBackup.sh secure
4. To encrypt changed database password parameters in the op-cc-backup-restore.env environment file, do the following steps:
 - a) Open a command or shell window on the reporting server.
 - b) Go to the <CC_Home>/tools/bin directory.
<CC_Home> is the installation location of Cognos.
 - For Microsoft Windows, <CC_Home> is C:\OpenPages\CommandCenter.
 - For Linux, <CC_Home> is opt/OpenPages/CommandCenter.
 - c) Type the following backup command:
 - On Windows: OPCCBackup.cmd secure
 - On Linux: ./OPCCBackup.sh secure

The OPBackup utility (Oracle)

OPBackup is the IBM OpenPages with Watson utility that backs up the necessary product files on the server where it is run. You can also use OPBackup to back up the database. The OPBackup utility creates a backup file that can be used by the OpenPages restore utility (OPRestore).

When you use the OPBackup utility, the following OpenPages with Watson resources are backed up:

- The OpenPages with Watson application
- The OpenPages with Watson storage folder and its content

- The OpenPages with Watson application environment files

You can also include the database in the backup. In a horizontal clustered environment, if you run OPBackup on a non-administrative server, the application database is not included in the backup. To include this database in a backup file, run OPBackup on an administrative server.

OPBackup does not back up standard tools by default. If you want to include additional files or directories, you must add them to a manifest file before you run the backup. For more information, see “Backing up custom files” on page 549.

Depending on your configuration, if any asynchronous background jobs are detected, the OPBackup job will exit and might display errors (see “Asynchronous background jobs and administrative functions” on page 547).

You can also configure email notification upon completion of an OPBackup. For details, see “Configuring backup job notification” on page 545.



Attention: If you have global search enabled, global search must be disabled before you run the OPBackup and OPRestore utilities. For more information, see “Using OPBackup and OPRestore when global search is enabled” on page 520.

Modifying the backup-restore environment file

The IBM OpenPages with Watson storage location is set during the installation process. Use the following scenarios to determine if you need to modify the OPSTORAGE_LOCATION parameter in the op-backup-restore.env file.

By default, the op-backup-restore.env file is located in the bin directory as follows: <OP_Home> | aurora | bin.

- For Microsoft Windows: <OP_Home> is C:\OpenPages.
- For Linux: <OP_Home> is /opt/OpenPages.

Scenario 1: The root installation path of the OpenPages with Watson storage location changed after installation

If you modify the root path of the IBM OpenPages with Watson storage location in the storageservers table after installation, make sure you update the OPSTORAGE_LOCATION parameter in the <OP_Home> | aurora | bin | op-backup-restore.env file to match the new root path (OpenPages with Watson storage location).

If these locations do not match, the OPBackup utility will capture incorrect or stale storage folders.

Scenario 2: The OPBackup utility is running on a non-administrative server

If you are running the OPBackup utility on a non-administrative server, you must update the OPSTORAGE_LOCATION parameter in the <OP_Home> | aurora | bin | op-backup-restore.env file on the non-administrative server to point to the remote location of the openpages_storage folder on the administrative server.

Make sure to use forward slashes as the path separator in this UNC path.

Example

```
//<host_server>/openpages_storage
```

Where:

<host_server> is the name of the administrative server.

Backing up custom files

You can include custom files, such as custom JSPs or other files that are specific to your environment, in backups by using a manifest file. A manifest file is a text file that contains the full path name to any directory or file that needs to be included in the backup.

For example, if you want to back up `openpages-ext.jar`, add its full path to the manifest file:

```
/opt/opuser/IBM/OpenPages/aurora/lib/openpages-ext.jar
```

Before you begin

- You must list all of your custom directories and files in a manifest. If you have any questions about the location of your custom data, contact IBM OpenPages Support.
- In a horizontal clustered environment, you must perform this procedure on each application server in the horizontal cluster.

Procedure

1. Log on to the application server.
2. If you have custom JSPs, do the following steps:
 - a) Create a zip file called `solutions-sosa-files.zip` that contains your custom JSPs and related files.

Tip: You can use a different name, but it must follow the convention `*-sosa-files.zip`. Also, you must add it to the `<OP_HOME>/aurora/bin/op-backup.manifest` file. Only `solutions-sosa-files.zip` is backed up and restored by default.
 - b) Put the `solutions-sosa-files.zip` file in the `<OP_HOME>/applications` directory.
 - When you run OPBackup, the zip file is included in the backup.
 - When you run OPRestore, the zip file is restored to `<OP_HOME>/applications` and is also extracted to `<OP_HOME>/wlp/usr/shared/apps/op-apps.ear/taskui.war/`
3. Open the `<OP_HOME>/aurora/bin/op-backup.manifest` file in a text editor.
4. Add custom files or directories, other than JSPs, to the `op_backup.manifest` file.

You can specify directories or individual files. For each file or directory, create a new line and type its full path..
5. Save the manifest file using the current location and name.

Running the OPBackup command (Oracle)

When you use the IBM OpenPages with Watson application backup utility, run the OPBackup command in a command or shell window.

The OPBackup command does the following:

- Stops all OpenPages with Watson services on the local application server before performing any backup operation
- Backs up OpenPages with Watson application and environment files
- Restarts the services on the local application server when the backup activities are complete

See “[Running a live backup \(Oracle\)](#)” on page 585 if you want to perform a backup without stopping services.

Procedure

1. If global search is enabled, disable it:
 - a) Log in to OpenPages as an administrator.

- b) Click  > **System Configuration** > **Global Search** and click **Disable**.
2. Shut down all non-admin application servers.
 3. Open a command or shell window on the OpenPages with Watson admin application server.
 4. Navigate to the `<OP_Home>/aurora/bin` directory.
 5. Run the following backup command:

Windows

```
OPBackup <path-to-backup-location>
```

Linux

```
./OPBackup.sh <path-to-backup-location>
```

Where `<path-to-backup-location>` is the full path of the directory where the backed up files are located on the OpenPages with Watson application server. If a file path is not specified, the OPBackup command uses the backup location that is specified in the BACKUP_LOCATION parameter of the `<OP_HOME>/aurora/bin/op-backup-restore.env` file.

You can use the following optional parameters:

- `app-nodb`: Back up everything except the OpenPages database.
- `dbonly`: Back up only the OpenPages database. (Applies to Oracle databases only.)

For example:

```
./OPBackup.sh <path-to-backup-location> app-nodb
```

Results

The backup process creates a log file in the `<backup-directory-name>` directory. Each time you run the OPBackup command, a separate log file is generated.

Backing up the OpenPages database (Oracle)

You can use the OPBackup utility to back up the IBM OpenPages with Watson databases.

About this task

Note: You can back up the databases by using other methods. Some examples of alternative methods include:

- Doing a full physical backup by using RMAN
- Doing a combination of full and incremental backup by using RMAN
- Doing an Oracle data pump export.

If you want to use an alternative method, it is critical that you have the necessary skills available within your organization to complete all aspects of the backup and restore activity.

Procedure

1. Make sure that no OpenPages with Watson processes are running, such as object reset jobs.
2. Shut down all OpenPages components: application servers (admin and non-admin), reporting servers (active and standby), and the search server.
For more information, see [Chapter 25, “Starting and stopping servers,” on page 709](#).
3. Open a command or shell window on the admin application server.
4. Go to the `<OP_HOME>/aurora/bin` directory.
5. Do a full database backup of the OpenPages schema by using OPBackup.

Windows:

```
OPBackup.cmd <backup_directory> dbonly
```

Linux:

```
./OPBackup.sh <backup_directory> dbonly
```

The *<backup_directory>* is the full path to a directory on the database server. This directory is where the log files are saved. If the file path is not specified, the OPBackup command uses the location that is specified by the **BACKUP_LOCATION** parameter in the *<OP_HOME>/aurora/bin/op-backup-restore.env* file.

A dump file is created in the **OP_DATAPUMP_DIRECTORY** directory.

6. Examine the backup log and make note of the dump file name. The naming convention is *openpage_<timestamp>.dmp*.

Running a live backup (Oracle)

A live IBM OpenPages with Watson backup means that the application can continue running while the backup is in progress. The services are not stopped during the backup.

Note: Run live OpenPages with Watson backups during off-peak hours because the backup consumes processing resources.

You might encounter errors such as the following during the database export portion of the live OP backup:

```
[exec] ORA-31693: Table data object "OPENPAGES"."table_name"  
      failed to load/unload and is being skipped due to error:  
[exec] ORA-02354: error in exporting/importing data  
[exec] ORA-01555: snapshot too old: rollback segment number #  
      with name "rollback_segment_name" too small
```

This might happen if there is a relatively high level of data modification transactional activity on the system during the backup. Run a live backup when transactional activity is low. If this is not possible or not desirable, or if the error keeps happening, it may be possible to avoid this error by setting **UNDO_RETENTION** initialization parameter to a higher (possibly much higher) value, at least for the duration of the backup. Setting **UNDO_RETENTION** to a higher value, may result in a growth of UNDO table space, so it should be done by an experienced database administrator or with the assistance of IBM OpenPages Support.

To use the OpenPages with Watson application backup utility live, you run the OPBackup command with the **nosrvrst** option. This does the following:

- Backs up OpenPages with Watson application and environment files
- Exports the OpenPages with Watson application database

Procedure

1. Open a command or shell window on the OpenPages with Watson admin application server.
2. Navigate to the *<OP_Home>/aurora/bin* directory.
3. Type the following backup command:

Windows

```
OPBackup <path-to-backup-location> nosrvrst
```

Linux

```
OPBackup.sh <path-to-backup-location> nosrvrst
```

where:

Windows

<path-to-backup-location> is <ORACLE_BASE>\admin\<SID>\dpdump

Linux

<path-to-backup-location> is <ORACLE_BASE>/admin/<SID>/dpdump

Results

The backup process creates a log file in the <backup-directory-name> directory. Each time you run the OPBackup command, a separate log file is generated.

OpenPages with Watson backed-up content

The backup process creates a ZIP file (.zip) in the <backup-directory-name> directory.

The ZIP file contains the following necessary backed up databases and data files:

- OpenPages application database
- OpenPages properties files (such as aurora.properties and Server<#>-sosa.properties).
- Application server configuration files for IBM WebSphere.
- The openpages-storage directory.
- Pointers to the database schema dump extracts.
- Files and directories that are listed in the manifest file (such as solutions-sosa-files.zip).

The manifest file is <OP_HOME>/aurora/bin/op-backup.manifest

Note:

- If a backup file is 4 GB or larger, configure the OPBackup utility to use gzip (GNU zip). Gzip produces an archive with an extension of .tar.gz. To view and extract the contents of the archive file, use WinZip 12 (or higher) or WinRAR 3.71 (or higher).
- The OPBackup utility adds a timestamp on the .zip and log files it creates.

The ZIP file can be used as a parameter to the OPRestore command to restore the installation-specific OpenPages with Watson files and the database. Each time the OPBackup command is run, a separate ZIP file is created and each data file is identified by a unique name.

Configuring OPBackup to use GZIP

If a ZIP backup file grows beyond the 4-GB limit of zip file capacity, you can configure the OPBackup utility to use gzip (GNU zip). After the file is configured, new backup files have a .tar.gz extension. The OPRestore utility detects if a file is in zip or gzip format and processes the file accordingly.

Procedure

1. From a command or shell window, navigate to the op-backup-restore.env file in the bin directory as follows.
 - For Windows, the installation directory is c:\<OP_Home>\aurora\bin
 - For Linux, the installation directory is <OP_Home>/aurora/bin
2. Open the op-backup-restore.env file in a text editor of your choice.
3. Change the USE_GZIP_COMPRESSION= setting from false to true.

Enabling and disabling storage backup

By default, the IBM OpenPages with Watson backup includes the storage folder and its content. You can disable storage backup by setting the BACKUP_OP_STORAGE parameter in the op-backup-restore.env file.

Procedure

1. Open a command or shell window on the OpenPages with Watson server.
2. Navigate to the op-backup-restore.env file in the bin directory as follows.

Table 178. Installation locations

Operating system	Installation location
Windows	<OP_HOME>\aurora\bin
Linux	<OP_HOME>/aurora/bin

3. Open the op-backup-restore.env file in a text editor of your choice.
4. Set the value of the BACKUP_OP_STORAGE parameter in the file to one of the following:

Table 179. BACKUP_OP_STORAGE parameter values and their meanings

If the value is set to...	Then...
true	The storage folder and its content are backed up. This is the default value.
false	The storage folder and its content are not backed up.

5. When finished, save the changes to the file and exit the editor.

The OpenPages restore utility on the Oracle database

OPRestore is the IBM OpenPages with Watson restore utility that restores the OpenPages files and database content on the server from which it was originally run. The OPRestore utility uses a backup file created by the OpenPages with Watson backup utility (OPBackup).

Important: To refresh a test environment, see [“Refreshing a test environment from backup files” on page 600](#).

As part of the restoration process, the following OpenPages with Watson resources are restored:

- The OpenPages with Watson application
- The OpenPages with Watson storage folder and its content
- The OpenPages with Watson application environment files

Important: In a horizontal environment, if OpenPages with Watson backup is run on a non-administrative server, the application database is not included in the backup, so will not be restored.

Depending on your configuration, an OPRestore job might not start until all asynchronous background jobs run to completion (see [“Asynchronous background jobs and administrative functions” on page 547](#)).

Running the OPRestore command (Oracle)

You can restore a backup using the OPRestore command. Use these steps if you're using Oracle.

Before you begin

If you used OPBackup, the zip file should contain the database dump files (.dmp). If the dump files are not in the zip file, copy them to the backup location before you start the restore.

Procedure

1. If you enabled the global search component during backup, re-create your search index so that your search results are synchronized.

- a) Click  > **System Configuration** > **Global Search** and click **Disable**.
 - b) Click **Drop** to drop the search indexes.
 - c) Click **Create** to re-create the search indexes.
2. Stop the IBM Cognos service.
 3. Shut down all non-admin application servers.
 4. On the admin application server, open a command or shell window.
 5. Navigate to the <OP_HOME>/aurora/bin directory.
 6. Run the following command:

Windows

```
OPRestore <backup-file-name> <path-to-backup-location>
```

Linux

```
./OPRestore.sh <backup-file-name> <path-to-backup-location>
```

Where <backup-file-name> is the name of the backup file (without the .zip or tar.gz file extension)

You can use the following optional parameters:

- **app-nodb**: Restore everything except the OpenPages database.
- **dbonly**: Restore only the OpenPages database. (Applies to Oracle databases only. To back up an IBM Db2 database, use the utilities that are provided with Db2.)

For example:

```
./OPRestore.sh <backup-file-name> <path-to-backup-location> app-nodb
```

What to do next

Preferences related to the long string text index won't be exported by “[Running the OPBackup command \(Oracle\)](#)” on page 583, and therefore are not restored. You must “[Create a long string index for an Oracle database](#)” on page 611 pointing to the database server you are restoring to.

OPRestore log files

The restore process creates a log file identified by a unique name in the <backup-directory-name> folder. Each time you run the OPRestore command, a separate log file is created.

Note: Oracle Data Pump log files for database imports are created on the database server.

Using the Cognos backup utility

OPCCBackup is the Cognos utility that backs up the necessary Cognos files. The OPCCBackup utility creates a backup file that can be used by the Cognos restore utility (OPCCRestore).

To back up or restore the IBM Db2 databases for IBM OpenPages with Watson, you must use the utilities that are provided with Db2. For more information about the databases in IBM OpenPages with Watson and backing up or restoring them, see “[Database backup and restore for OpenPages \(Db2\)](#)” on page 555.

When you use the OPCCBackup utility, the following Cognos resources are backed up.

- Cognos reports
- Branding and environment files

You can configure email notification (with an attached log file) upon the completion of an OPCCBackup. For details, see “[Configuring backup job notification](#)” on page 545.

Oracle Data Pump configuration on a first time use

Before you use the Cognos backup utility for the first time, you must configure Oracle Data Pump by running an SQL script.

This task is required.

For details on running the script, see [“Configuring or updating the Oracle Data Pump directory” on page 589.](#)

The script configures a data pump storage directory for the user name specified in the <user_name> parameter. If a datapump storage directory was already configured for the specified user name, the script will display an appropriate message.

The OpenPages with Watson file storage directory

By default, OP_DATAPUMP_DIRECTORY is the name of the directory used for storing Cognos Content Store database backup files. The path to this directory on the database server varies and depends on how it was defined.

If the OP_DATAPUMP_DIRECTORY storage directory does not already exist on the database server, you must run the script to create the directory.

Configuring or updating the Oracle Data Pump directory

The script used in this procedure requires access to the content of the installation kit:
OP_<version>_Main.

Use the following SQL*Plus script to:

- Create the Oracle Data Pump datapump directory for first time use of the CommandCenter backup utility.
- Update configuration information if you modified the log file name or datapump directory location to reflect changes in your environment.

Procedure

1. Log on to a machine with SQL*Plus and a connection to the CommandCenter database instance.
2. Open a command or shell window.
3. Go to the following directory:

/OP_<version>_Main/OP_<version>_Configuration/Database/ORACLE/
UPGRADE_SCRIPTS

4. Run the update-datapump-directory.sql script as follows and substitute values for each parameter:

```
sqlplus /nolog @sql-wrapper update-datapump-directory <log_file_name>  
<tns_name_alias> SYSTEM <password> <create|update> <directory_location>  
<user_name>
```

Note: All parameters are required.

Table 180. Parameters for Oracle Data Pump SQL script

This parameter...	Represents...
<log_file_name>	The user-defined name of the log file that the script will create and write information to. Examples Linux: /tmp/update-datapump.log Windows C:\temp\update-datapump.log

Table 180. Parameters for Oracle Data Pump SQL script (continued)

This parameter...	Represents...
<tns_name_alias>	The database Oracle TNS entry to be used by the OpenPages CommandCenter database instance on the reporting server computer.
<password>	The password for the Oracle SYSTEM user account. If the password contains special characters, surround the password in quotation marks: <ul style="list-style-type: none">• Windows: "password"• Linux: 'password'
<create update>	Specify one of the following values: <ul style="list-style-type: none">• create - use this if you are configuring Data Pump for first time use.• update - use this if you are modifying the <Directory Location> parameter.
<directory_location>	The full directory path on the database server where the backed up files will be placed.
<user_name>	The user name to be used with the Cognos account for the CommandCenter database schema (Content Store).

Example:

```
sqlplus /nolog @sql-wrapper update-datapump-directory.sql C:\temp\update-datapump.log
OP SYSTEM "password" create d:\cc_backup cognos
```

```
sqlplus /nolog @sql-wrapper update-datapump-directory.sql /tmp/log
op SYSTEM 'password' create TESTDIR openpage
```

Running the OPCCBackup command

When you use the Cognos backup utility, you run the OPCCBackup command in a command or shell window. The OPCCBackup command uses Oracle Data Pump to export the database (services can continue to run during the backup).

Note: Oracle Data Pump backup files are created on the database server.

Procedure

- From a command or shell window, navigate to the <CC_Home>/tools/bin, where <CC_Home> represents the installation location of the Cognos application.
- Run the following backup command:

Windows

```
OPCCBackup <path-to-backup-location>
```

Linux

```
OPCCBackup.sh <path-to-backup-location>
```

Where:

<path-to-backup-location> is the full path of a backup directory on the Cognos server. The file path is optional.

Note: If no file path is specified, the OPCCBackup command uses, by default, the backup location that is specified in the BACKUP_LOCATION parameter of the <CC_Home>|tools|bin|op-cc-backup-restore.env file.

The default content store database export locations are:

- Windows: <oracle_base>\admin\<SID>\dpdump
- Linux: <oracle_base>/admin/<SID>/dpdump

If you get the warning tools.jar file is not found, see the following [technote](#).

Results

The backup process creates a log file in the <backup-directory-name> folder. Each time you run the OPCCBackup command, a separate log file is generated.

Cognos backed-up content

The Cognos backup process creates a ZIP file (.zip) in the <backup-directory-name> directory. This ZIP file contains the necessary report and environment files that can be used by the Cognos restore utility (OPCCRestore).

Note:

- If a backup file is very large (4 GB or larger), configure the OPCCBackup utility to use gzip (GNU zip). Gzip produces an archive with an extension of .tar.gz. To view and extract the contents of the archive file, use WinZip 12 (or higher) or WinRAR 3.71 (or higher).
- The OPCCBackup utility adds a military timestamp on the .zip and log files it creates.

The ZIP file can be used as a parameter to the OPCCRestore command to restore the installation-specific IBM OpenPages with Watson files and the database. Each time the OPCCBackup command is run, a separate ZIP file is created and each data file is identified by a unique name.

Configuring OPCCBackup to use GZIP

If a ZIP backup file grows beyond the 4-GB limit of ZIP file capacity, you can configure the OPCCBackup utility to use gzip (GNU zip). When the file is configured, new backup files have a .tar.gz extension. The OPCCRestore utility detects if a file is in zip or gzip format and processes it accordingly.

Procedure

1. From a command or shell window, locate the op-cc-backup-restore.env file in the <CC_Home>/tools/bin directory, where <CC_Home> represents the installation location of the Cognos application.
 - For Windows, the default location of <CC_Home> is C:\OpenPages\CommandCenter.
 - For Linux, the default location of <CC_Home> is /opt/OpenPages/CommandCenter.
2. Open the op-cc-backup-restore.env file in a text editor.
3. Change the **USE_GZIP_COMPRESSION=** setting in the file from false to true.

Using the Cognos restore utility

OPCCRestore is the IBM OpenPages with Watson Cognos utility that restores the necessary Cognos files and Content Store on the server from which it was originally run. The OPCCRestore utility uses a backup file created by the OpenPages with Watson Cognos backup utility (OPCCBackup).

Note: To refresh a "test" environment, see ["Refreshing a test environment from backup files" on page 600](#).

As part of the restoration process, the following Cognos resources are restored:

- Cognos reports

- Content Store
- Branding and environment files

Running the OPCCRestore command

You can restore backed up Cognos data using the OPCCRestore utility as follows.

Procedure

1. Stop the IBM Cognos service on the administrative server and any non-administrative servers in the cluster. For details, see [“Starting and stopping the Cognos services” on page 717](#).
2. Stop the IBM Cognos Configuration tool, if it is running, on all cluster members.
3. From a command or shell window, navigate to the <CC_Home>/tools/bin directory where <CC_Home> represents the installation location of the Cognos application.
 - For Windows, the installation location is C:\OpenPages\CommandCenter.
 - For Linux, the installation location is /opt/OpenPages/CommandCenter
4. On the administrative Cognos server, run the following command:

Windows

```
OPCCRestore <backup-file-name> <path-to-backup-location>
```

Linux

```
OPCCRestore.sh <backup-file-name> <path-to-backup-location>
```

Where:

<backup-file-name> is the name of the backup file (without the .zip or tar.gz file extension).

Note: <path-to-backup-location> is the full path of the directory where the backed up files are located on the Cognos server. The file path is optional.

If no file path is specified, the OPCCRestore command uses, by default, the backup location specified in the BACKUP_LOCATION parameter of the <CC_Home>|tools|bin|op-cc-backup-restore.env file.

5. Start the IBM Cognos service on the administrative server and on any non-administrative servers in the cluster. For details, see [“Starting and stopping the Cognos services” on page 717](#).

Results

The restore process creates a log file identified by a unique name in the <backup-directory-name> folder. Each time you run the OPCCRestore command, a separate log file is created.

Note: Oracle Data Pump log files for database imports are created on the database server.

Using Oracle online database backup (RMAN) for point-in-time recovery

To perform an online backup of the IBM OpenPages with Watson database, using custom OpenPages scripts that use Oracle’s Recovery Manager (RMAN) facility.

Knowledge of basic Oracle database backup and recovery operations is necessary, as well as use of RMAN. For more information on the use of RMAN for online database backup and recovery, see the Oracle documentation.

Oracle online database backups

Unlike the IBM OpenPages with Watson OPBackup utility, the Oracle online database backup function does not require shutting down access to database operations before backing up the database.

It can perform an incremental backup in the background at a designated interval while allowing full user access to the OpenPages with Watson database and OpenPages with Watson services. It also allows "point in time" recovery of the OpenPages with Watson database with minimal chance of data loss.

In contrast, OPBackup and OPRestore can only do a full backup and restore of the database and other files (not incremental). Because full backups are typically performed less frequently than incremental backups, the possibility of significant data loss in the event of a system crash is greater than for the Oracle online database backup and recovery solution.

Note:

- The Oracle online database backup function can only perform a physical bit-for-bit backup of a single OpenPages with Watson database instance and only on one machine.
- Operation of online database backup in an Oracle RAC (cluster) environment is not supported.

In contrast, OPBackup performs a logical backup of all database instances in the cluster, as well as the OpenPages with Watson storage directory and application environment files.

Running Oracle online database backups (RMAN)

Setting up and running Oracle online database backups has several steps.

Complete the following steps to set up and run Oracle online database backups:

["Plan the size of the Oracle backup area" on page 593](#)

["Copying the online Oracle backup scripts to a local directory" on page 594](#)

["Modifying the environment variables in the Oracle RMAN-ENV script" on page 594](#)

["Configure the Oracle database for online backup" on page 596](#)

["Run the Oracle rman-daily script" on page 597](#)

Plan the size of the Oracle backup area

The backup area is the location where the Oracle online database backup function stores the backup copy of the database instance plus the redo logs and other database-related files.

The online redo log represents the currently running incremental database backup, and the archived redo logs represent previous incremental backups. Estimate the maximum size of the backup area in order to set the appropriate environment variable. For more information, see ["Modifying the environment variables in the Oracle RMAN-ENV script" on page 594](#).

As a guideline, use a backup area that is 3x the size of the database. It includes the sum of the database, database copy, and archived log files.

The size of the backup area must be large enough to store all of the following information:

- A copy of the database instance
- All online redo logs
- Any archived redo logs that have not been backed up elsewhere.
- A copy of the database control file and the SPFILE

The backup area should be able to store at least 24 hours of archived redo logs that have not been backed up.

Copying the online Oracle backup scripts to a local directory

To access the scripts for online database backup, copy them from the installation media, OP_<version>_Main, to any local directory on the database server. You can run the scripts from the local directory.

Procedure

1. Log on to the IBM OpenPages with Watson database server as a user with administrative privileges.
2. Open a command or shell window.
3. Go to the following directory:
`/OP_<version>_Main/OP_<version>_Configuration/Database/ORACLE/
INSTALL_SCRIPTS`
4. From the INSTALL_SCRIPTS directory copy, the following scripts to a local directory on the database server.
 - Environment-specific online backup scripts:

Windows

```
    rman-env.cmd  
  
    rman-init.cmd  
  
    rman-daily.cmd  
  
    recover-db.cmd
```

Linux

```
    rman-env.sh  
  
    rman-init.sh  
  
    rman-daily.sh  
  
    recover-db.sh
```

- More online backup scripts:

```
enable-archivelog-mode.sql  
disable-archivelog-mode.sql  
check-fra-size.sql  
load_OP_APP_DATA.sql  
no-op.sql  
sql-wrapper.sql  
update-fra-size.sql  
init_recovery_env.sql
```

Note:

- The name of the local directory where you are copying the scripts must not contain any space characters.
- You can run the scripts described in the following topics from the local directory. You can add the directory to your PATH environment variable so that you can run them from any directory.

Modifying the environment variables in the Oracle RMAN-ENV script

After you determine the size of the backup area, edit the environment variable values in the `rman-env` script.

Before you begin

Complete the following steps to modify the Oracle RMAN-ENV script:

Procedure

1. Open the `rman-env.cmd` (Windows) or `rman-env.sh` (Linux) script in a text editor on the database server. Edit the following environment variables for your Oracle database environment as shown in Table 181 on page 595.

Table 181. Environment Variables in RMAN-ENV Script

Environment Variable	Description
<code>ORACLE_HOST_NAME=</code>	Fully qualified network identifier for the database server computer. The hostname can be found in the HOST parameter in the <code>tnsnames.ora</code> file. Example: <code>mydbhost.openpages.com</code>
<code>ORACLE_SID=</code>	SID of the IBM OpenPages database instance you are backing up. The SID can be found in the SERVICE_NAME parameter in the <code>tnsnames.ora</code> file. Example: <code>op</code>
<code>ORACLE_HOME=</code>	The Oracle database Home directory on the database server where the Oracle software is installed, including the database. This is the same as the value of the <code><ORACLE_HOME></code> environment variable for the database server. Examples Database and application servers on the same machine: Windows <code>C:\openpages_data\repository\server112_se_x64\software</code> Linux <code>/opt/oracle/openpages_data/repository/server112_se_x64/software</code> Database and application servers on different machines: Windows <code>C:\openpages_data\repository\client112_ac_x64\software</code> Linux <code>/opt/oracle/openpages_data/repository/client112_ac_x64/software</code>
<code>ORACLE_DATAFILE_LOC=</code>	The Oracle data Home directory on the database server. This is the location where the Oracle data is stored. Examples Windows <code>C:\openpages_data\repository\database112_se_x64\oradata\<server_name></code> Linux <code>opt/openpages_data/repository/database112_se_x64/oradata/<server_name></code>

Table 181. Environment Variables in RMAN-ENV Script (continued)

Environment Variable	Description
FLASH_RECOVERY_AREA=	Directory or file system where the backup area will be located on the database server. Example: c :\temp\arch (Windows)
FLASH_RECOVERY_AREA_SIZE=	Maximum size of the backup area, specified in either megabytes (M) or gigabytes (G). You can specify any size up to the maximum allowed by the operating system on the database server. Examples: <ul style="list-style-type: none"> • 500M (500 megabytes) • 20G (20 gigabytes)
LISTENER_PORT=	Listener port number of the Oracle database instance you are backing up. The listener port number can be found in the PORT parameter in the tnsnames.ora file. Example: 1521
ORACLE_HOME_NAME=	Name assigned to <ORACLE_HOME> at installation time. The Oracle Home Name can be found in the SERVER parameter in the inventory.xml file in the <Oracle_Home>\Inventory\ContentsXML directory. Example: OPServer

2. Save the script file.

Results

After you enable online backup mode for a database instance, do not make any changes to the corresponding rman-env script. If you need to increase the size of the backup area, see “[Adjusting the size of the Oracle backup area](#)” on page 598 for more information. Never modify the rman-env script to adjust the size of the backup area after online database backup mode is enabled.

If you need to back up a different database instance, make a copy of the rman-env script in a different directory and modify the parameters as appropriate. The FLASH_RECOVERY_AREA parameter must specify a different location than that of your other online database backups.

Configure the Oracle database for online backup

Run the rman-init script to create the required directories and scripts for database recovery and to configure the parameters that you entered in the rman-env script for Oracle online database backup.

To run the script, execute the following command:

Windows

```
rman-init.cmd <tns_name_alias> SYS "<sysdba_password>"
```

Linux

```
rman-init.sh <tns_name_alias> SYS '<sysdba_password>'
```

Where:

<tns_name_alias> is the TNS alias of the IBM OpenPages with Watson database instance as it is known on the network. If necessary, you can retrieve this alias from the tnsnames.ora file.

<sysdba_password> is the Oracle SYS account password.

Windows example

```
rman-init op SYS "password"
```

If there are errors when running this script, the script output will list the directory location containing the error log. The error log file name is enable-archivelog-more.log.

Important: The script described in this section restarts the database. It is recommended that you alert users that they will be temporarily unable to access the database until the script has finished running.

Run the Oracle rman-daily script

The rman-daily script can be run manually or on a scheduled basis by using standard operating system scheduler functions (such as cron).

After you configure the database for online backup, you can run the rman-daily script to perform online backups.

Run the following command:

Windows

```
rman-daily.cmd <tns_name_alias> SYS "<sysdba_password>"
```

Linux

```
rman-daily.sh <tns_name_alias> SYS '<sysdba_password>'
```

Where:

<tns_name_alias> is the TNS alias of the IBM OpenPages with Watson database instance as it is known on the network. If necessary, you can retrieve this alias from the tnsnames.ora file.

<sysdba_password> is the Oracle SYS account password.

Linux example

```
rman-daily.sh op SYS 'password'
```

Review Oracle log files

The rman-daily script produces a log file (rman-daily.log) that lists each component that was backed up. The log is re-created (overwritten) each time that you run the rman-daily script.

The directory location of the rman-daily.log is:

Windows

```
<FLASH_RECOVERY_AREA>\<ORACLE_SID>\logs
```

Linux

```
<FLASH_RECOVERY_AREA>/<ORACLE_SID>/logs
```

Where:

<FLASH_RECOVERY_AREA> and <ORACLE_SID> are the values of those parameters in the rman-env script.

The log file lists the following information for the online database backup:

- Backup sets (incremental backups)
- Copies of data files

- Copies of control files
- Temp files

Monitoring the size of the Oracle backup area

You can use a script to monitor the size of the backup area.

To monitor and display the size of the backup area, use the following script:

```
sqlplus /nolog @sql-wrapper check-fra-size.sql <log_file_name> <tns_name_alias>
        SYSTEM <system_password>
```

Where:

- <log_file_name> is the directory location, including the log file name that you specify, where any errors or messages relating to this script are logged. If you specify only the log file name, it is stored in the current working directory.
- <tns_name_alias> is the TNS alias of the IBM OpenPages with Watson database instance as it is known on the network. If necessary, you can retrieve this alias from the tnsnames.ora file.
- <system_password> is the Oracle SYSTEM account password.

If the password contains special characters, surround the password in quotation marks:

- Windows: "password"
- Linux: 'password'

The script displays the following information (in megabytes):

- Used Space — Space that is already used and not available for online database backups.
- Allocated Space — Maximum size of the backup area, including used and free space. This is the same as the value of the FLASH_RECOVERY_AREA_SIZE parameter in the rman-env script.
- Used-Reclaimable — Space that is free for use in online database backups.

Example: Displays the used, allocated, and free space for the database instance op.

- Windows:

```
sqlplus /nolog @sql-wrapper check-fra-size.sql C:\OpenPages\logs op SYSTEM "password"
```

- Linux:

```
sqlplus /nolog @sql-wrapper check-fra-size.sql /tmp/log op SYSTEM 'password'
```

Adjusting the size of the Oracle backup area

You can adjust the size of the backup area if necessary.

Occasionally, you may need to modify the size of the backup area. For example, you may see the following warning message in the Oracle Alert log:

```
ORA-19815: WARNING: db_recovery_file_dest_size of xxxx bytes is 100.00% used,
and has 0 remaining bytes available
```

Increase the size of the backup area to make more space available for online database backups. You can increase or decrease the size of the backup area by running one of the scripts described in the following section.

Important: Do not delete files manually from the backup area to free up space. Doing so causes the following error: RMAN-06059: expected archived log not found.

Reclaiming used space by running the Oracle rman-daily script

Running the `rman-daily` script reclaims previously used space in the backup area, freeing it up for use in online database backups.

Adjusting space by running the Oracle UPDATE-FRA-SIZE script

You can adjust the size of the backup area by using a script.

If you want to adjust the maximum size of the backup area to a specific value, run the following scripts. The `enable-archivelog-mode.sql` script enables archive log mode, which enables Oracle online database backup for the specified database instance. The `update-fra-size.sql` script adjusts the size of the online backup area.

```
sqlplus /nolog @sql-wrapper enable-archivelog-mode.sql <log_file_name> <tns_name_alias>
  sys <sysdba_password> <archive_dir> <file_size>
sqlplus /nolog @sql-wrapper update-fra-size.sql <log_file_name> <tns_name_alias>
  SYS <sysdba_password> <new_size>
```

Where:

- `<log_file_name>` is the directory location, including the log file name that you specify, where any errors or messages relating to this script are logged. If you specify only the log file name, it is stored in the current working directory.
- `<tns_name_alias>` is the TNS alias of the IBM OpenPages with Watson database instance as it is known on the network. If necessary, you can retrieve this alias from the `tnsnames.ora` file.
- `<sysdba_password>` is the Oracle SYS account password.

If the password contains special characters, surround the password in quotation marks:

- Windows: "password"
- Linux: 'password'
- `<archive_dir>` is the directory where the archive file is stored.
- `<file_size>` is the maximum size of the archive file.
- `<new_size>` is the updated size of the backup area (use M for megabytes or G for gigabytes). For example, you would specify 20 gigabytes as 20G.

Example: Enables archive log mode and then sets the backup area for the database instance op to 1 gigabyte.

- Windows:

```
sqlplus /nolog @sql-wrapper enable-archivelog-mode.sql c:\tmp\log OP sys
  "password" c:\tmp 50M
sqlplus /nolog @sql-wrapper update-fra-size.sql C:\temp\log op SYS "password" 1G
```

- Linux:

```
sqlplus /nolog @sql-wrapper enable-archivelog-mode.sql /tmp/log OP sys
  'password' /tmp/ 50M
sqlplus /nolog @sql-wrapper update-fra-size.sql /tmp/log OP sys 'password' 1G
```

Important: The script restarts the database. Users are unable to access the database while the script is running.

Disabling online backup of the Oracle database instance

Run the following script to turn off archive logging mode, which disables Oracle online database backup for the specified database instance.

This simply stops the service that runs online database backup; it does not remove any files or data already stored in the backup area.

```
sqlplus /nolog @sql-wrapper disable-archivelog-mode <log_file_name> <tns_name_alias>
SYS <sysdba_password>
```

Where:

- <log_file_name> is the directory location, including the log file name that you specify, where any errors or messages relating to this script are logged. If you specify only the log file name, it is stored in the current working directory.
- <tns_name_alias> is the TNS alias of the IBM OpenPages with Watson database instance as it is known on the network. If necessary, you can retrieve this alias from the `tnsnames.ora` file.
- <sysdba_password> is the Oracle SYS account password.

If the password contains special characters, surround the password in quotation marks:

- Windows: "password"
- Linux: 'password'

Example: Disables online backup for the database instance op.

- Windows:

```
sqlplus /nolog @sql-wrapper disable-archivelog-mode c:\tmp\log op SYS "password"
```

- Linux:

```
sqlplus /nolog @sql-wrapper disable-archivelog-mode /tmp/log op SYS 'password'
```

Important:

- The script restarts the database. Users are unable access the database while the script is running.
- After disabling online database backup mode, if you want to re-enable online database backup mode for the database instance, do not use the `rman-init` or `rman-daily` scripts. Doing so may cause unpredictable database behavior or other problems. To re-enable online database backup mode, contact IBM OpenPages Support for assistance.

Performing Oracle online database crash recoveries

If a system crash or other problem either corrupts the database instance or causes it to fail, the database must be recovered from the online backup.

The actual recovery procedure may vary depending on the nature of the crash, which parts of the database were damaged, and your system environment. For that reason, database recoveries must only be performed by IBM OpenPages Support.

Refreshing a test environment from backup files

To refresh an existing test (target) environment, you can replicate it from a production (source) environment. By using backup files from a production environment, you can update a test environment that closely matches your production environment.

Note: Oracle Data Pump backup files are created on the database server.

Prerequisites

Ensure you have access to the production server and test server.

Ensure the production server and test server have the same installed version of IBM OpenPages with Watson, including patches.

Ensure you have access to the installation media: OP_<version>_Main

Backing up and copying the OpenPages with Watson application production files for an Oracle database

The exported data from the production backup file will be used later to refresh data on the test server.

Procedure

1. Log on to your production IBM OpenPages with Watson server as a user with administrative permissions.
2. Run the OpenPages with Watson backup utility (OPBackup) to back up the OpenPages application database.
For more information, see [“The OPBackup utility \(Oracle\)” on page 581](#).
3. Copy the backup .zip or .tar.gz file to your test server.

Backing up the OpenPages with Watson application test files on your Oracle test data

You can back up IBM OpenPages with Watson application test data.

Procedure

1. Log on to your test OpenPages with Watson server as a user with administrative permissions.
2. Run the backup utility (OPBackup) as described in [“The OPBackup utility \(Oracle\)” on page 581](#) to backup the OpenPages with Watson application database.

Deleting data on the test database system

You can delete data on the test database system.

Procedure

1. If necessary, log on to your IBM OpenPages with Watson test server as a user with administrative permissions.
2. Open a command or shell window.
3. Go to the following directory:
`/OP_<version>_Main/OP_<version>_Configuration/Database/ORACLE/
INSTALL_SCRIPTS`
4. From the INSTALL_SCRIPTS directory, run the AuroraDbDelete.sql script as follows:
 - a) Log on to SQL*Plus as the OpenPages with Watson database user (for example: sqlplus openpages/openpages@test).
 - b) Run the following script to drop the objects in the schema on the test server:
`@AuroraDbDelete.sql`
 - c) When finished, log out of SQL*Plus.

Copy the production database dump (.dmp) file to the test database server

You can copy the production database file to the test database server.

Procedure

1. Locate the database dump (.dmp) file directory on the source production and target test database servers.

Note:

To find the datapump directory for either the source or target database, run the following SQL query as the system user:

```
select directory_name, directory_path from dba_directories  
where directory_name = upper ('OP_DATAPUMP_DIRECTORY');
```

By default, the datapump directory on the database server is <oracle-server-directory>|admin|<sid>|dpdump

2. Copy the IBM OpenPages with Watson database dump (.dmp) file from the Oracle datapump directory on the production database server to the datapump directory on the test database server.

Table 182. Default file name for .dmp file

For this .dmp file...	The default file name will be similar to this...
OpenPages with Watson	OPENPAGES_<timestamp>.DMP

Note: Make sure to copy the .dmp file with the timestamp that matches when you ran the OPBackup command.

Import the production data into the test environment

You must import the IBM OpenPages with Watson database.

Procedure

1. Open a command or shell window and set the NLS_LANG environment variable as follows.

Windows

In the Command Prompt window where you will be invoking the import commands, execute the following command:

```
set NLS_LANG=AMERICAN_AMERICA.AL32UTF8
```

Linux

Open the .profile file in the logged in user's home directory in a text editor and enter the following line if it is missing in the file:

```
export NLS_LANG=AMERICAN_AMERICA.AL32UTF8
```

Save the change to the file, and either execute the .profile in your shell window or log on again.

2. Import the OpenPages database on the test database server from the backup files in “Backing up and copying the OpenPages with Watson application production files for an Oracle database” on page 601 as follows.

Note: The Oracle Data Pump command IMPDP is used as the IMP command is not supported.

For more information on Oracle Data Pump, see “Oracle Data Pump” on page 577.

From the same command or shell window, run the following command to import the OpenPages database:

```
impdp <op_db_user>/\"<op_db_password>\\"@<SID>  
DIRECTORY=OP_DATAPUMP_DIRECTORY DUMPFILE=<openpages_dump_file>  
LOGFILE=openpages_import.log
```

Table 183. Parameters and their descriptions

Parameter	Description
<op_db_user>	The user name for accessing the OpenPages database.
<op_db_password>	The password for accessing the OpenPages database.
<SID>	The Oracle System Identifier (for example, OP or OP).
<openpages_dump_file>	<p>The .dmp file name of the backed up OpenPages with Watson application database.</p> <p>Important: Do not enter an explicit path when specifying the .dmp file name. Enter only the file name.</p>
DIRECTORY	<p>The directory on the database server where the backed up files will be placed. This is set when “Configuring or updating the Oracle Data Pump directory” on page 589.</p> <p>Important: Do not enter an explicit path when specifying the DIRECTORY parameter. Use OP_DATAPUMP_DIRECTORY only.</p>

Example

```
impdp openpages/"openpages"@OP
DIRECTORY=OP_DATAPUMP_DIRECTORY DUMPFILE=openpages_backup_YYYY_MM_DD_HH_MI_SS.dmp
LOGFILE=openpages_import.log
```

Note: If the source schema name and target schema names are different, the schema must be remapped during import. Add the following argument to this impdp command to remap the schema:

```
Remap_schema=<source_schema>:<target_schema>
```

Example

```
impdp openpages/"openpages"@OP
DIRECTORY=OP_DATAPUMP_DIRECTORY DUMPFILE=openpages_backup_YYYY_MM_DD_HH_MI_SS.dmp
LOGFILE=openpages_import.log remap_schema=opuser:openpages
```

Update the OpenPages with Watson storage location in the Oracle database

After you restore the **openpage-storage** file from the product backup, you must update the IBM OpenPages with Watson storage location in the database.

Procedure

1. Log on to a system with administrative permissions. You can use any system with access to CLPPlus that can connect to the OpenPages database server.
2. Copy all the files under the openpages-storage folder from the production backup .zip file to the openpages-storage location on the test server.

By default, the storage location is <OP_Home>|openpages-storage

Table 184. Installation location of the OpenPages with Watson application

Operating system	Installation location
Windows	For example, <OP_HOME> C:\IBM\OpenPages
Linux	For example, <OP_HOME> /opt/IBM/OpenPages

3. Open a command or shell window and go to the following directory:
 /OP_<version>_Main/OP_<version>_Configuration/Database/ORACLE/
 INSTALL_SCRIPTS
4. From the INSTALL_SCRIPTS directory, run the update-storage SQL wrapper script with the following parameters (see [Table 185 on page 604](#) for a description) to update the openpages-storage directory location in the database:

```
sqlplus /nolog @sql-wrapper.sql update-storage <log-file> <oracle_tns_alias>
<op_db_user> <op_db_password> <storage-type> <storage-server-name>
<host-name> <os-type> <path-or-UNC-name>
```

Where:

Table 185. Update Storage Wrapper Script Parameters

Parameter	Description
<log-file>	The name of the log file that the script will create and write information to.
<oracle_tns_alias>	The database alias for the OpenPages with Watson database instance, as set during the Oracle database installation.
<op_db_user>	The OpenPages with Watson user name for accessing the OpenPages with Watson database.
<op_db_password>	The OpenPages with Watson password for accessing the OpenPages with Watson database. If the password contains special characters, surround the password in quotation marks: <ul style="list-style-type: none"> • Windows: "password" • Linux: 'password'
<storage-type>	The type of file storage to be used. Valid values are: <ul style="list-style-type: none"> • LFS (local file system) • UNC (Universal Naming Convention) Note: After you move from LFS to UNC, you cannot go back to using LFS.
<storage-server-name>	The name of the storage server.
<host-name>	The hostname of the machine.
<os-type>	The type of operating system. Valid values are: <ul style="list-style-type: none"> • Windows • Unix
<path-or-UNC-name>	The file path or UNC of the storage location.

Examples

- LFS

Windows

```
sqlplus /nolog @sql-wrapper.sql
update-storage c:\temp\upd-storage-output.log
op openpages "password" LFS eng11 eng11
Windows c:\OpenPages\openpages-storage
```

Linux

```
sqlplus /nolog @sql-wrapper.sql
update-storage /home/op/upd-storage-output.log
op openpages 'password' LFS eng11 eng11
Unix /usr/opdata/openpages-storage
```

- UNC

Windows

```
sqlplus /nolog @sql-wrapper.sql
update-storage c:\temp\update-storage-output.log
op openpages "password" UNC eng11
eng11 Windows openpages-storage
```

Update the global search settings

After you import data from a production environment (the source environment) into a test or development environment (the target environment), you need to update the global search settings.

About this task

When you import data from the source environment, the settings for the search server are imported. You need to update the target environment so that it uses the search server in your target environment.

Procedure

1. Log in to the OpenPages application in the target environment as a user with administrative privileges.
2. Click  > **System Configuration** > **Global Search** and click **Disable**.
3. Stop the global search services.
For more information, see “[Start or stop the global search services](#)” on page 712.
4. Update the global search settings.
 - a) Click **System Configuration** > **Settings** > **Applications** > **Common** > **Configuration** > **Show Hidden Settings** and set the value to true.
 - b) Click **System Configuration** > **Settings** > **Platform** > **Search** > **Admin** and update the **Search Server Administration URL** with the URL of the search server in your target environment.
 - c) Click **System Configuration** > **Settings** > **Platform** > **Search** > **Index** and update the **Search Server URL** with the URL of the search server in your target environment.
 - d) Click **System Configuration** > **Settings** > **Platform** > **Search** > **Request** and update the **Search Server URL** with the URL of the search server in your target environment.
5. Copy the `<SEARCH_HOME>/openpages-solr-index` directory to the search server in the target environment.
The `<SEARCH_HOME>/openpages-solr-index` contains the global search index.
6. Start the global search services.
For more information, see “[Start or stop the global search services](#)” on page 712.
7. Click  > **System Configuration** > **Global Search** and click **Enable**.

Results

Global search is enabled in the target environment.

Update Cognos data in the test environment

You can update Cognos data in the test environment by using the Cognos backup utility.

Before you begin

Before you run the Cognos backup utility (OPCCBackup) make sure to verify the following:

- You have access to both the source and target database servers.
- The <CC_user> has Read and Write permission to the OP_DATAPUMP_DIRECTORY.

Where: <CC_user> is the name of the Cognos content store database user.

If not, you must grant the proper permissions on both the production and test servers to the <CC_user> account on the datapump directory as follows:

1. Log on to a machine with SQL*Plus and access to the database server.
2. Run the following SQL command as the system user:

```
grant read,write on directory OP_DATAPUMP_DIRECTORY to <CC-user>;
```

- Full permission is granted to the CommandCenter|tools|bin folder on the target Cognos server.

Backup Cognos production Oracle data and files

The exported data from the production backup file will be used later to refresh data on the test server.

Procedure

1. If necessary, log on to your production Cognos server as a user with administrative permissions.
2. Run the Cognos backup utility (OPCCBackup) to back up the Cognos database and configuration files.

For more information, see “[Using the Cognos backup utility](#)” on page 588.

Tip: If the mail server for notification e-mails has not been set up for running Cognos backups, the output from the OPCCBackup command might end with the following error:

```
BUILD FAILED
c:\machine3\CommandCenter\tools\bin\op-cc-backup-email-notification.xml:31:
  Problem while sending mime mail:
```

This error can be safely ignored as long as this step says BUILD SUCCESSFUL.

3. Copy the production Cognos server backup .zip or .tar.gz file to the Cognos backup-restore directory on the test server.
4. Copy the database dump (.dmp) file from the Oracle datapump directory on the source database server to the datapump directory on the target database server.

Make sure you copy the dump file with the timestamp that matches when you ran the OPCCBackup command. By default, the file will be named similar to OPENPAGES_CC_<timestamp>.DMP.

Note:

To find the datapump directory for either the source or target database, run the following SQL query as the system user:

```
select directory_name, directory_path from dba_directories
where directory_name = upper ('OP_DATAPUMP_DIRECTORY');
```

By default, the datapump directory on the database server is <oracle-server-directory>|admin|<sid>|dpdump

Backing up the Cognos Oracle test data and files

You can back up test data and files.

Procedure

1. If necessary, log on to your test IBM OpenPages with Watson server as a user with administrative permissions.
2. Run the Cognos backup utility (OPCCBackup) as described in “[Using the Cognos backup utility](#)” on [page 588](#) to back up the Cognos database and configuration files.

Restoring the Cognos data and files to the Oracle test environment

You can restore data and files to the test environment.

Procedure

1. Log on to your test IBM OpenPages with Watson server as a user with administrative permissions.
2. From the INSTALL_SCRIPTS directory, run the AuroraDbDelete.sql script as follows:
 - a) Log on to SQL*Plus as the Cognos database user (for example: sqlplus cognos/cognos@test).
 - b) Run the following script to drop the objects in the schema on the test server:
 @AuroraDbDelete.sql
 - c) When finished, log out of SQL*Plus.
3. Import the Cognos database on the target (test) database server from the backup file from the source (production) database server as follows.

From a command or shell window, run the following command to import the Cognos database:

```
impdp <cognos_db_user>/<cognos_db_password>@<SID>
DIRECTORY=OP_DATAPUMP_DIRECTORY
DUMPFILE=<cc_dump_file> LOGFILE=cc_import.log
```

Where:

Table 186. Parameters and their descriptions

Parameter	Description
<cognos_db_user>	The Cognos user name for accessing the Cognos database.
<cognos_db_password>	The Cognos password for accessing the Cognos database.
<SID>	The Oracle System Identifier (for example, OP).
<cc_dump_file>	The .dmp file name of the backed up Cognos database.

Example

```
impdp cognos/"cognos"@OP DIRECTORY=OP_DATAPUMP_DIRECTORY
DUMPFILE=openpages_cc_YYYY_MM_DD_HH_MI_SS.dmp
LOGFILE=openpages_cc_import.log
```

Note: If the source schema name and target schema names are different, the schema must be remapped during import. Add the following argument to this impdp command to remap the schema:

```
Remap_schema=<source_schema>:<target_schema>
```

Example

```
impdp cognos/"cognos"\@OP DIRECTORY=OP_DATAPUMP_DIRECTORY  
DUMPFILE=openpages_cc_YYYY_MM_DD_HH_MI_SS.dmp  
LOGFILE=openpages_cc_import.log remap_schema=cognos8:cognos
```

Change password references for Oracle data sources

The following procedure describes how to manually update the sign-on password for the user account to access data sources.

Depending on the type of installation, one or both of the following Oracle data source links are displayed in the IBM Cognos Administration tool for the reporting framework:

- The **OpenPages DataSource** is used for the reporting framework.

Note: For Oracle Database environments only, both the **OpenPages DataSource** and **Oracle Native Driver** data sources connect to the same database repository and use the same authentication information (sign-ons).

Procedure

1. From a browser, log on to the IBM Cognos Analytics as a user with administrative privileges, for example, OpenPagesAdministrator.

By default, the URL is `http://<hostname>/ibmcognos/bi`
Where <hostname> is the name of the Cognos server.
2. Click **Manage > Administration Console** to launch the **IBM Cognos Administration** page.
3. On the **Configuration** tab, click **Data Source Connections** (if not already selected).
4. On the **Directory > Cognos** page, click the **More** link in the same row as the data source you want (for example, OpenPages DataSource).
5. On the **Perform an Action** page, under **Available actions**, click the **View connections** link.
6. On the **Directory > Cognos > < name of data source >** page, click the **More** link in the same row as the selected data source.
7. On the **Perform an Action** page for the data source, under **Available actions**, click the **View signons** link.
8. On the **Directory > Cognos > < name of data source > signons** page, do the following:
 - a) Under the **Actions** column, click the **Set properties - < name of data source >**  icon.
 - b) On the **Set properties-< name of data source >** page, click the **Signon** tab.
9. On the **Signon** tab:
 - a) Click the **Edit the signon** link.
 - b) Update the password.

Updating Oracle database connection references for reports

You can update the database connection references for reports.

Procedure

1. From a browser, log on to IBM Cognos Analytics as a user with administrative privileges, for example, OpenPagesAdministrator.

By default, the URL is:

`http://<hostname>/ibmcognos/bi` (if you are using port 80 for Cognos)

Where <hostname> is the name of the Cognos server.

2. Click **Manage > Administration Console** to launch the **IBM Cognos Administration** page.
3. On the **Configuration** tab, click **Data Source Connections** (if not already selected).
4. On the **Directory > Cognos** page, click the link for the IBM OpenPages with Watson data source.
5. On the **Directory > Cognos > OpenPages DataSource** page, do the following:
 - a) Under the **Actions** column, click the **Set properties - OpenPages DataSource** icon 
 - b) On the **Set properties - OpenPages DataSource** page, click the **Connection** tab.
6. On the **Connection** tab, next to the **Connection String** box, click the pencil icon to edit the field.
7. On the edit page, do the following:
 - a) On the **OCI** tab, in the **SQL*Net connect string** box, change the SQL*Net connect string to the TNS alias of the OpenPages database on the target environment.
 - b) On the **JDBC** tab, in the **Server name**, **Port number**, and **Oracle Service ID** boxes, change the values to valid values for the IBM OpenPages with Watson database on the target environment.
8. If this is an upgraded legacy system, repeat the steps in this task for the **Oracle Native Driver**, if it exists.

Modify SSO and LDAP Configuration in the test environment

If you are using SSO and/or LDAP in the test environment, modify the configuration for each if needed. Otherwise, skip this task.

Copy custom triggers

You must copy any custom Java actions and triggers that have been deployed on the production server to the test environment. These custom actions and triggers are added to a zip file, `openpages-ext.jar`, by the OPBackup utility.

If you have any questions about the location of your custom data, contact IBM OpenPages Support.

Procedure

1. If necessary, log on to your test IBM OpenPages with Watson server as a user with administrative permissions.
2. Update the `openpages-ext.jar` in the test environment as follows:
 - a) From the production backup .zip file, navigate to the `openpages-ext.jar` in the `<OP_Home>|aurora|lib` directory.

Where `<OP_HOME>` represents the installation location of the IBM OpenPages application.

Table 187. Installation location of the OpenPages with Watson application

Operating system	Installation location
Windows	<code><OP_HOME>\aurora\lib\openpages-ext.jar</code> By default <code><OP_HOME></code> is <code>C:\IBM\OpenPages</code>
Linux	<code><OP_HOME>/aurora/lib/openpages-ext.jar</code> By default <code><OP_HOME></code> is <code>/opt/IBM/OpenPages</code>

- b) Copy the `openpages-ext.jar` from the production backup file into the `<OP_Home>|aurora|lib` directory on your test machine and overwrite the existing `.jar` file there.

Copy other custom deliverables to the test environment

If you have other custom deliverables, such as UI helpers and JSP reports, copy these custom deliverables to their respective folders on the test or target machine.

If you have any questions about the location of your custom data, contact IBM OpenPages Support.

Procedure

1. From your application production backup .zip files, extract all custom files such as JAR files, JSP files, JavaScript files, and Image files.
2. Copy these files into their respective folders on the target machine. The target folders should match the folders on the source installation.

Starting OpenPages with Watson in the test environment

When finished, start IBM OpenPages with Watson services on the servers in your test environment.

For details, see [Chapter 25, “Starting and stopping servers,” on page 709](#).

Updating the OPSystem password

If the OPSystem password is different in the source (production) and target (test) environments or if you changed the default OPSystem password, update the OPSystem password in the test environment.

For more information, see [“Changing the OPSystem password” on page 637](#).

Update URL host pointers for Cognos reports

Modify the URL host pointer settings and then propagate these changes to the reporting schema on the application server (does not require services to be restarted).

For more information, see [“Updating URL host pointers for reports” on page 633](#).

Utilities for filtering on long string field content in an Oracle database

You can filter based on the content of long string fields if the Oracle Text feature has been enabled. This is also known as full text searching.



Warning: Do not include long string fields that are encrypted using field level encryption in the search criteria because they can return unexpected results.

Long string fields allow users to enter values over 4KB in length. To apply filters on the content of these long string fields, first [“Enabling Oracle Text” on page 612](#) feature. If the Oracle Text feature is not enabled, attempts to filter on the content of long string fields will generate errors. For details on setting up long text fields, see [“Long String data type” on page 157](#).

There are five utilities provided to help manage full text searching:

- [“Enabling Oracle Text” on page 612](#)
- [“Create a long string index for an Oracle database” on page 611](#)
- [“Create a schedule job to synchronize a long string index” on page 613](#)
- [“Drop a long string index” on page 614](#)
- [“Modifying the list of stop words” on page 615](#)

To apply filters with long string fields, you must change the **OpenPages > Platform > Database > Text Indexes** setting to **true**.

Table 188. Values and what they mean

If the value is set to...	Then...
true	Filtering is enabled on long string fields.
false	Filtering is disabled on long string fields. The default is false .

For details on working with settings, see [Chapter 20, “Viewing the Configuration and Settings page,” on page 473](#).

Create a long string index for an Oracle database

Create a long string text index to support filtering based on the contents of fields with long string data types. Scripts are provided for both Windows and Linux.

Before you begin

Oracle Text must be enabled. See [“Enabling Oracle Text” on page 612](#).

Procedure

1. Log on to a system as a user with Administrator privileges. You can use any system with access to SQL*Plus that can connect to the IBM OpenPages with Watson database server.
2. Open a command or shell window, navigate to the `full-text-index` directory as follows.

The following table identifies the installation location of the application on the Microsoft Windows and Linux operating systems.

Table 189. Installation location of the full-text-index directory

Operating system	Installation location
Windows	<code><OP_HOME>\aurora\bin\full-text-index</code>
Linux	<code><OP_HOME>/aurora/bin/full-text-index</code>

Note: If the database server is not on the same computer as the OpenPages server, you must copy the script, and the SQL files it starts, to the database server.

3. Run the following batch command:

Windows

```
CreateOpenPagesTextIndex.bat <SID> <OPX_USER_NAME>
"<OPX_USER_PASSWORD>" <MEMORY_LIMIT> <PARALLEL_INDEXING_DEGREE>
```

Linux

```
CreateOpenPagesTextIndex.sh <SID> <OPX_USER_NAME>
'<OPX_USER_PASSWORD>' <MEMORY_LIMIT> <PARALLEL_INDEXING_DEGREE>
```

Table 190. Parameters

Parameter name	Description
<code><SID></code>	The system ID or TNS alias for the OpenPages database instance.
<code><OPX_USER_NAME></code>	OpenPages database schema owner name.
<code><OPX_USER_PASSWORD></code>	OpenPages database schema owner password.

Table 190. Parameters (continued)

Parameter name	Description
<MEMORY_LIMIT>	Specifies the amount of runtime memory to use for indexing, in megabyte or gigabyte values. For example, valid values include 128M and 2G.
<PARALLEL_INDEXING_DEGREE>	Parallel degree for parallel indexing. The actual degree of parallelism might be smaller depending on system resources.

Enabling Oracle Text

Enable the Oracle Text feature to filter based on the contents of fields with long string data types. Scripts are provided for Windows and Linux.

Procedure

1. Log on to the Oracle database server as a user with database administrator privileges.

Note: You can enable Oracle Text only from the database server.

2. Open a command or shell window, navigate to the `full-text-index` directory as follows.

The following table identifies the installation location of the application on the Microsoft Windows and Linux operating systems.

Table 191. Installation location of the full-text-index directory

Operating system	Installation location
Windows	<code><OP_HOME>\aurora\bin\full-text-index</code>
Linux	<code><OP_HOME>/aurora/bin/full-text-index</code>

Note: If the database server is not on the same computer as the IBM OpenPages with Watson server, copy the script and the SQL files to the database server.

3. Run the following batch command:

Windows

```
EnableOpenPagesTextIndexing.bat <SID> <SYSDBA_USER_NAME>
  '<SYSDBA_PASSWORD>' <OPX_USER_NAME>
```

Linux

```
EnableOpenPagesTextIndexing.sh <SID> <SYSDBA_USER_NAME>
  '<SYSDBA_PASSWORD>' <OPX_USER_NAME>
```

Note: All parameters are required.

Table 192. Parameters in the batch command

Parameter name	Description
<SID>	The system ID or TNS alias for the OpenPages with Watson database instance.
<SYSDBA_USER_NAME>	Database SYSDBA account. Usually the SYS user.
<SYSDBA_PASSWORD>	Password for the SYSDBA user account.
<OPX_USER_NAME>	OpenPages with Watson application schema owner name.

Results

The database is now enabled for indexing. Use “Create a long string index for an Oracle database” on page 611 script to create the index.

Create a schedule job to synchronize a long string index

Create a schedule to synchronize the long string index. Scripts are provided for both Windows and Linux.

Procedure

1. Log on to a system as a user with Administrator privileges. You can use any system with access to SQL*Plus that can connect to the IBM OpenPages with Watson database server.
2. Open a command or shell window, then navigate to the full-text-index directory as follows.

The following table identifies the installation location of the application on the Microsoft Windows and Linux operating systems.

Table 193. Installation location of the full-text-index directory

Operating system	Installation location
Windows	<OP_HOME>\aurora\bin\full-text-index
Linux	<OP_HOME>/aurora/bin/full-text-index

Note: If the database server is not on the same machine as the OpenPages server, you must copy the script, and the SQL files it invokes, to the database server.

3. Run the following batch command:

Windows

```
ManageOpenPagesTextIndexRefreshJob.bat <SID> <OPX_USER_NAME>
'<OPX_USER_PASSWORD>' <START_JOBS_AFTER_DAYS> <JOB_START_HOUR> <REFRESH_FREQ_IN_HOURS>
<REFRESH_FREQ_IN_MINS> <MEMORY_LIMIT> <PARALLEL_INDEXING_DEGREE> <MAX_SYNC_TIME>
```

Linux

```
ManageOpenPagesTextIndexRefreshJob.sh <SID> <OPX_USER_NAME>
'<OPX_USER_PASSWORD>' <START_JOBS_AFTER_DAYS> <JOB_START_HOUR> <REFRESH_FREQ_IN_HOURS>
<REFRESH_FREQ_IN_MINS> <MEMORY_LIMIT> <PARALLEL_INDEXING_DEGREE> <MAX_SYNC_TIME>
```

Table 194. Parameters

Parameter name	Description
<SID>	The system ID or TNS alias for the OpenPages database instance.
<OPX_USER_NAME>	OpenPages database schema owner name.
<OPX_USER_PASSWORD>	OpenPages database schema owner password.
<START_JOBS_AFTER_DAYS>	Number of days between today and the scheduled starting date of the job. For example, 0 for today, 1 for tomorrow.
<JOB_START_HOUR>	The hour (on a 24-hour clock) of the scheduled starting date of the job. For example, 18 for 1800 hours or 6 p.m.
<REFRESH_FREQ_IN_HOURS>	Intervals (in hours) between each job. This value is combined with <REFRESH_FREQ_IN_MINS> value. Maximum of combined values is 999.

Table 194. Parameters (continued)

Parameter name	Description
<REFRESH_FREQ_IN_MINS>	Intervals (in minutes) between each job. This value is combined with <REFRESH_FREQ_IN_HOURS>. Maximum of combined values is 999.
<MEMORY_LIMIT>	Specifies the amount of runtime memory to use for indexing, in megabyte or gigabyte values. For example, valid values include 128M and 2G.
<PARALLEL_INDEXING_DEGREE>	Parallel degree for parallel indexing. The actual degree of parallelism might be smaller depending on system resources.
<MAX_SYNC_TIME>	Maximum time (in minutes) the index synchronization job can run.

Results

Index synchronization jobs run at the interval specified.

Note: Changes to long string fields are not available for filtering until the next scheduled index job runs.

For example, ManageOpenPagesTextIndexRefreshJob.bat OP opadmin "opadmin" 1 3 24 0 2G 0 60 schedules indexing synchronization to start at 3 AM. starting on the next day, and then repeats every day at the same time. There is a 2-gigabyte memory limit, no parallel indexing, and the job can run no more than an hour.

Drop a long string index

Remove the long string index. An index must be dropped before it can be re-created. Scripts are provided for both Windows and Linux.

Procedure

1. Log on to a system as a user with Administrator privileges. You can use any system with access to SQL*Plus that can connect to the IBM OpenPages with Watson database server.
2. Open a command or shell window, then navigate to the full-text-index directory as follows.

The following table identifies the installation location of the application on the Microsoft Windows and Linux operating systems.

Table 195. Installation location of the full-text-index directory

Operating system	Installation location
Windows	<OP_HOME>\aurora\bin\full-text-index
Linux	<OP_HOME>/aurora/bin/full-text-index

Note: If the database server is not on the same machine as the OpenPages server, you must copy the script, and the SQL files it invokes, to the database server.

3. Run the following command:

Windows

```
DropOpenPagesTextIndex.bat <SID> <OPX_USER_NAME> "<OPX_USER_PASSWORD>"
```

Linux

```
DropOpenPagesTextIndex.sh <SID> <OPX_USER_NAME> '<OPX_USER_PASSWORD>'
```

Table 196. Parameters	
Parameter name	Description
<SID>	The system ID or TNS alias for the OpenPages database instance.
<OPX_USER_NAME>	OpenPages database schema owner name.
<OPX_USER_PASSWORD>	OpenPages database schema owner password.

What to do next

You must re-create the index before filtering on the content of long string fields again. For details on creating a long string index, see [“Create a long string index for an Oracle database” on page 611](#).

Modifying the list of stop words

You can change the default list of stop words used by the Oracle Text feature. A stop word is a word that does not get indexed. When querying an Oracle Text index for a stop word, Oracle Text won’t return data for the query.

By default, the `CreateOpenPagesTextIndex.bat | .sh` script creates a stop word list called `OP_STOPLIST`. (See [“Create a long string index for an Oracle database” on page 611](#).) The stop word list is empty at the time of index creation.

You can use the `CustomIndexing_ManageStopWords.sql` script to add stop words to `OP_STOPLIST`.

Procedure

1. Open `CustomIndexing_ManageStopWords.sql` with a text editor
2. Add a stop word for each word you would like to add by copying the following, commented out sections:

```
/*
  ADD_STOPWORD_TO_ARRAY
  (
    p_name          => 'me'
  );
*/
```

For example, if you want to add the stop word “the”, copy the preceding section, remove the comment sign, and replace “me” with “the” as follows. Repeat the same step for each word you want to add.

```
ADD_STOPWORD_TO_ARRAY
(
  p_name          => 'the'
);
```

Stop words that you add to this file take effect the next time that you re-index. This file is used as the most updated list of stop words when the index is re-created. When running `CustomIndexing_Step2_IndexCreate.sql`, all current stop words in `OP_STOPLIST` are removed. It is a good idea to keep this file up to date.

String concatenation utility

String concatenation lets you merge up to 8 simple strings into a new long text field (long string data type). Long text fields have two sub categories - medium long and large long. Medium long can support a text size up to 32KB.

To concatenate simple strings, the fields must be unencrypted. After you use the concatenation utility, you can encrypt the new long text field.

You must log in as an administrator to perform string concatenation. You can use any system with access to SQL*Plus that can connect to the IBM OpenPages with Watson database server.

String concatenation is a database operation. A SQL template file is provided to specify parameters for the action. For more information, see [“Running string concatenation” on page 616](#).

For more information on long text fields, see [“Long String data type” on page 157](#).

Running string concatenation

The string concatenation utility runs an SQL file that you edit to provide input and output parameters.

Important:

- The string concatenation utility puts the system into System Administration Mode (SAM) prior to concatenating any fields. No other activity can happen while the script is running.
- You can concatenate into an existing long text field, but only if that field has not been used in any way. Attempting to concatenate into a long text field that has been used causes the utility to fail.
- When you concatenate multiple strings, if field level security is applied to any of the strings, then after concatenation into a single, large long text field, some hidden values can be visible. To prevent unauthorized users from viewing the values for a concatenated string, apply the same field level security rule to the large long text field.

Tip: Run the script in preview mode (a setting in the `field_concat_template.sql` file) to check the results before doing the concatenation.

Procedure

1. Log on to a system as a user with Administrator privileges. You can use any system with access to SQL*Plus that can connect to the IBM OpenPages with Watson database server.
2. Stop all services (see [Chapter 25, “Starting and stopping servers,” on page 709](#)).
3. Navigate to the `field-concat-utility` folder located in the `bin` directory:

Table 197. Installation locations

Operating system	Installation location
Windows	<code><OP_HOME>\aurora\bin</code>
Linux	<code><OP_HOME>/aurora/bin</code>

4. Copy the contents of the SQL template `field_concat_template.sql` into a new file.
5. Edit the new SQL file to provide the values necessary. Edit only the values in the declaration section of the SQL file. For details, see [“The string concatenation SQL file” on page 617](#).

Important: Many of the parameters specified in the SQL file have requirements, restrictions, and cautions noted. These are important for a successful concatenation.

Tip: When editing your copy of the `field_concat_template.sql` file with multi-byte characters, and saving the file in Unicode, your editor may insert a Byte Order Mark (BOM) into the file. Some applications (such as a text editor or a browser) display the BOM as an extra line in the file, while others display unexpected characters, such as `\u202e`. If you save the file in UTF-8 encoding (leaving the BOM in the file) and run the string concatenation script, you get an error message (SP2-0734:

unknown command beginning "ï»¿-----..."), but the script continues to run without a problem. This error has no effect on the script running, but if you prefer not to see the error, save the file without a Byte Order Mark.

6. Run the following command:

Windows

```
field_concat <SID> <op_db_user> "<op_db_password>"  
<field_concat_template_file>
```

Linux

```
field_concat.sh <SID> <op_db_user> '<op_db_password>'  
<field_concat_template_file>
```

Table 198. Parameters

Parameter name	Description
<SID>	The system ID or TNS alias for the OpenPages database instance.
<username>	The OpenPages database schema user name.
<password>	The OpenPages database schema owner password. If the password contains special characters, surround the password in quotation marks: <ul style="list-style-type: none">• Windows: "password"• Linux: 'password'
<field_concat_template_file>	The name of the SQL file created in step 3.

Tip: To see details on database operation messages, run the following SQL statement:

```
select exception_text from error_messages where  
ERROR_MESSAGE_ID = &ERROR_MESSAGE_ID;
```

7. Start all services (see [Chapter 25, “Starting and stopping servers,” on page 709](#)).
8. Optional: Apply a field level security rule to the large long text field. For more information, see [“Field level security” on page 92](#).

Results

If the destination long text field does not exist, it is created and populated with values according to the values specified in the SQL file.

If the destination long text field exists, but is not used in any way, it is populated with values according to the values specified in the SQL file.

For details on the SQL file, see [“The string concatenation SQL file” on page 617](#).

The string concatenation SQL file

IBM OpenPages with Watson includes a template SQL file (`field_concat_template.sql`). Use a copy of this file to specify the parameters to submit with the `field_concat` command.

Important: Many of the parameters specified in the SQL file have requirements, restrictions, and cautions noted. These are important for a successful concatenation.

See [“Running string concatenation” on page 616](#).

Parameters

Table 199. *field_concat_template.sql* parameters

Parameter	Description
l_actor_name	The user name making the change. The user must log in as an administrator. The script puts the system into System Administration Mode (SAM) prior to concatenating any fields.
l_field_group_name_src<#>	<p>The name of the field group containing the simple string field.</p> <p>Where: <#> is a value from 01 to 08.</p> <ul style="list-style-type: none"> • l_field_group_name_src<#> and l_property_name_src<#> are always specified in pairs. • These parameters must have values specified in order. For example, l_field_group_name_src01 must have a value before l_field_group_name_src02 is specified. • Specified field groups must be associated with an object type.
l_property_name_src<#>	<p>The name of the source simple string field.</p> <p>Where: <#> is a value from 01 to 08.</p> <ul style="list-style-type: none"> • The source must be a simple string. • At least one source must be specified. • The source must already exist • l_field_group_name_src<#> and l_property_name_src<#> are always specified in pairs. • These parameters must have values specified in order. For example, l_property_name_src01 must have a value before l_property_name_src02 is specified. • A property can only be specified once in the set of fields to concatenate. • Only the resource description system property is supported.

Table 199. *field_concat_template.sql* parameters (continued)

Parameter	Description
l_separator	<p>The separator to use between concatenated fields. The default separator is null.</p> <p>If you concatenate only one source into the destination, the separator character is not used.</p> <ul style="list-style-type: none"> • To use "&" as a separator, encode it as <code>chr(38)</code>. <p>For example:</p> <pre>l_separator OP_GLOBALS.DB_Max_String_T := chr(38);</pre> <ul style="list-style-type: none"> • The separator string can be no longer than 100 bytes. • If the destination field has a rich text display type, characters in the separator sequence must be encoded. <p>For example, to represent a less-than sign ("<"), encode it as:</p> <pre>l_separator OP_GLOBALS.DB_Max_String_T := chr(38) 'lt';</pre>
l_object_type_name	<p>The name of the object type containing the destination long text field.</p> <p>The object type must be the same for the destination as it is for the source.</p>
l_field_group_name	<p>The name of the field group containing the destination long text field.</p> <ul style="list-style-type: none"> • The destination field group must exist. • The destination field group must be a customer field group, not a system field group.
l_property_name	<p>The name of the destination field.</p> <ul style="list-style-type: none"> • The name destination field must either not exist, or if it does exist, must not used anywhere. • If the destination field does not already exist, the <code>l_large_text_length</code> parameter must be specified. • If the destination field does exist, it must be of data type Long String. • If the destination field is Rich Text, and source fields are a mix of Text and Rich Text, then there is the possibility that the concatenated value will not display properly in the UI. Such operations should be executed with caution.
l_property_desc	The description of the destination long text field.

Table 199. `field_concat_template.sql` parameters (continued)

Parameter	Description
<code>l_large_text_length</code>	The length property of the destination field. The default is <code>OP_OBJ_MODEL_MGR.g_dl_longtext_medium</code> . If the destination does not exist, this parameter must be specified, as either <code>OP_OBJ_MODEL_MGR.g_dl_longtext_medium</code> or <code>OP_OBJ_MODEL_MGR.g_dl_longtext_large</code> .
<code>l_is_done_by_vendor</code>	Set to true to add the concatenation to audit trail. The default is <code>OP_Globals.sc_False</code> . Valid values are: <ul style="list-style-type: none"> • <code>OP_Globals.sc_True</code> • <code>OP_Globals.sc_False</code> See “ Auditing configuration changes ” on page 634
<code>l_remote_address</code>	The remote address to perform the audit trail. The default is null. Any value is ignored if <code>l_is_done_by_vendor</code> is <code>OP_Globals.sc_False</code> .
<code>l_remote_host</code>	The remote host to perform the audit trail. The default is null. Any value is ignored if <code>l_is_done_by_vendor</code> is <code>OP_Globals.sc_False</code> .
<code>l_preview_only</code>	Set to true to only print the changes that will be made by script. No changes are actually made. The default is <code>OP_Globals.sc_False</code> . Valid values are: <ul style="list-style-type: none"> • <code>OP_Globals.sc_True</code> • <code>OP_Globals.sc_False</code> Tip: Run the script in preview mode (a setting in the <code>field_concat_template.sql</code> file) to check the results before doing the concatenation.

Table 199. *field_concat_template.sql* parameters (continued)

Parameter	Description
l_override_objtp_logic	<p>Set to true to override any logic applied to the object types, such as their relationships. The default is OP_Globals.sc_False.</p> <p>Valid values are:</p> <ul style="list-style-type: none"> • OP_Globals.sc_True • OP_Globals.sc_False <p>If l_object_type_name is left blank, and the source and destination field groups are associated to different object types, the script will fail unless you set this parameter to OP_Globals.sc_True. Each source field group and destination field group must associate with the same object type or set of object types.</p> <p>For example, the following scenario will fail unless this parameter is set to OP_Globals.sc_True:</p> <ul style="list-style-type: none"> • Source field group A is associated to object types X and Y. • Source field group B is associated only to object type X. • Destination field group is associated only to object type X.

Sample

Note: The following sample includes only those declarative statements that are subject to your changes.

```

declare
  l_actor_name          ACTORINFO.NAME%type           := 'OPAdmin';
  l_field_group_name_src01 BUNDLEDEFS.NAME%type       := 'QA10_SS_1';
  l_property_name_src01  PROPERTYDEFS.NAME%type       := 'QA10_Simple2';
  l_field_group_name_src02 BUNDLEDEFS.NAME%type       := 'QA10_LargeText';
  l_property_name_src02  PROPERTYDEFS.NAME%type       := 'QA10_S3';
  l_field_group_name_src03 BUNDLEDEFS.NAME%type       := 'Core Attributes';
  l_property_name_src03  PROPERTYDEFS.NAME%type       := 'Resource Description';
  l_field_group_name_src04 BUNDLEDEFS.NAME%type       := 'MG_7';
  l_property_name_src04  PROPERTYDEFS.NAME%type       := 'MG_S7';
  l_field_group_name_src05 BUNDLEDEFS.NAME%type       := 'MG_4';
  l_property_name_src05  PROPERTYDEFS.NAME%type       := 'MG_S4';
  l_field_group_name_src06 BUNDLEDEFS.NAME%type       := 'MG_5';
  l_property_name_src06  PROPERTYDEFS.NAME%type       := 'MG_S5';
  l_field_group_name_src07 BUNDLEDEFS.NAME%type       := 'MG_6';
  l_property_name_src07  PROPERTYDEFS.NAME%type       := 'MG_S6';
  l_field_group_name_src08 BUNDLEDEFS.NAME%type       := 'MG_3';
  l_property_name_src08  PROPERTYDEFS.NAME%type       := 'MG_S3';
  l_separator            OP_GLOBALS.DB_Max_String_T  := '';
  l_object_type_name     ASSETTYPES.NAME%type        := 'SOXBusEntity';
  l_field_group_name     BUNDLEDEFS.NAME%type        := 'QA10_LargeText';
  l_property_name        PROPERTYDEFS.NAME%type       := 'TEST101';
  l_property_desc        PROPERTYDEFS.DESCRIPTION%type:= 'MGMGMGMGDescription';
  l_large_text_length    PROPERTYDEFS.DATA_LENGTH%type:=
OP_OBJ_MODEL_MGR.g_dl_longtext_medium;
  l_is_done_by_vendor    OP_Globals.Flag_String_T   := OP_Globals.sc_False;
  l_remote_address       i18n_audit_trail.remote_address%type := '';
  l_remote_host          i18n_audit_trail.remote_host%type  := '';
  l_preview_only         OP_Globals.Flag_String_T   := OP_Globals.sc_False;
  l_override_objtp_logic OP_Globals.Flag_String_T   := OP_Globals.sc_False;
```

Entity Move/Rename utility

The IBM OpenPages with Watson Entity Move/Rename utility allows batch processing of multiple Business Entities for overnight or weekend execution without running the risk of operations that time out. You can run the utility interactively or as a scheduled job.

Using the Entity Move/Rename utility, you can do the following:

- Rename a Business Entity hierarchy
- Simultaneously rename and move a Business Entity hierarchy

A single batch job can contain multiple independent operations, multiple dependent operations, or any combination thereof.

Each operation provides transactional consistency. If an operation fails, all the pending changes for this operation are rolled back. If an operation succeeds, all the changes are persisted.

Each rename, move, or combined operation runs in its own transactional context. So, failure in one operation does not result in the failure of the entire batch job.



CAUTION: Before running the utility, you must stop all application services to avoid data or security errors.

Entity Move/Rename utility prerequisites

Before you use the IBM OpenPages with Watson Entity Move/Rename utility, consider these prerequisites.

- A physical computer or VM that meets the OpenPages with Watson installation requirements. For detailed specifications, see the *IBM OpenPages with Watson Installation and Deployment Guide*.
- An application that produces either CSV (comma-separated value) files or Unicode tab delimited files. This application can be installed on any computer in your environment and is used to prepare the input data for the utility.
- User name and password for the Oracle or IBM Db2 account that owns the OpenPages application database schema (for example, OPENPAGES).

Configuring the Entity Move/Rename utility for an Oracle database

You must configure parameters in the OpenPages with Watson Entity Move/Rename utility before you use it in an Oracle database environment.

Procedure

1. Go to the Entity Move/Rename utility installation location as follows:

OP_Home\aurora\bin\batch_entity_move_rename_relative

2. Open the *batch-entity-move-rename.ini* configuration file for editing.

3. Specify appropriate values in the following parameters for an Oracle database environment:

Table 200. Parameters for an Oracle database in the batch-entity-move-rename.ini file:

Parameter Name	Description
connect_string	Oracle database connection details. Use either the TNS alias or EZCONNECT format. TNS: <user>/<password>@<TNS alias> EZCONNECT: <user>/<password>@//<host>:<port>/<sid>

Table 200. Parameters for an Oracle database in the batch-entity-move-rename.ini file:
(continued)

Parameter Name	Description
data_format	<p>Format of the input file to the utility.</p> <p>Example: csv or unicode-text</p> <p>Use the csv file format as follows:</p> <ul style="list-style-type: none"> Only if the data is known to contain ASCII characters exclusively. All the national characters in the data input file are produced from the same Windows or ISO code page that is configured on the computer. You must specify the correct Oracle character set name that matches the code page in the character_set parameter.
input_file	<p>Name of the input file (including extension).</p> <p>Example: 'Sample-batch-entity-move-rename.txt'</p>
character_set	<p>ANSI/ISO character set that is used by the utility.</p> <p>If the data_format parameter is set to csv, you must use a correct Oracle character set name that corresponds to the ANSI/ISO code page used by the OS (such as, WE8MSWIN1252).</p> <p>If the data_format parameter is set to unicode-text, this parameter is ignored.</p>
skip_rows	<p>The number of rows in the input files to skip on load.</p> <p>Example</p> <p>If the first row of the file:</p> <ul style="list-style-type: none"> Contains a list of column names, set the value to '1'. Does not contain a list of column names, set this value to '0'.

- Save and close the batch-entity-move-rename.ini configuration file.
- Prepare the input file. See ["Prepare the input file for the Entity Move/Rename utility" on page 574](#).

Prepare the input file for the Entity Move/Rename utility

The input file for the Entity Move/Rename utility can be in CSV or Unicode tab delimited format. You can use any editor to create the input files. Included in the utility installation folder is a sample Unicode text file (.txt format).

Important: On Linux, the text input file must be saved or converted to be encoded in UCS-2 LittleEndian and have Linux end of line (LF) characters.

Tip: If you are using Microsoft Excel, you must save the spreadsheet as a CSV or tab delimited file.

The input file must have the following five columns of data:

Table 201. Columns in the input file

Column Name	Description	Sample Value
Source entity location	The entity on which the operation is run.	/The Bank/USA/North East/Providence

Table 201. Columns in the input file (continued)

Column Name	Description	Sample Value
Target entity location	The new parent entity for "move" and "move and rename" operations only. Note: <ul style="list-style-type: none"> For Oracle "rename" operations only (no move), the value must be "-" (dash). For Db2 "rename" operations only (no move), the value must be blank. 	For "move" and "move and rename" operations: /Worldwide/ Americas/USA/NE
Run as user	Application user name, whose identity is used to run the operation.	OpenPagesAdministrator
New entity name	The new name after the operation for "rename" and "move and rename" operations only. Note: <ul style="list-style-type: none"> For Oracle "move" operations only (no rename), the value must be "-" (dash). For Db2 "move" operations only (no rename), the value must be blank. 	For "rename" and "move and rename" operations: Boston
Execution order	Establishes the operation execution order as follows: <ul style="list-style-type: none"> Operations that specify the execution order are run before operations that do not. Operations that have a numeric value in the execution order column are run in regular ascending ordering. If set, the value must be a valid number; Otherwise, leave the field blank.	1

The following is a short description of the data in the sample .txt file that is included in the utility directory.

- The first line illustrates moving entity /The Bank/USA/North East/Providence to new location /Worldwide/Americas/USA/NE. Operation is to be run as the user SOXAdministrator. This operation is run first in the batch.
- The second line illustrates in place rename of the entity /Worldwide/Americas/USA/NE/ Providence. Entity name changes to Boston. Target location does not apply and is set to "-". This entry has a dependency on the previous move operation and has higher number in the execution order column. Also, it references to the new entity location that will be in effect after the first operation completes.
- If the first operation fails for any reason, this operation fails as well and the entity location would be incorrect.
- The third line illustrates simultaneous move of the entity /The Bank/USA/Midwest/Chicago to new location /Worldwide/Americas/USA/MW and rename to Detroit. This operation has no dependencies and will be run after the first two complete.

If you have an Oracle database with the 32-bit SQL*Loader utility in a Linux environment, see the topic: ["Avoid error 0509-036 when you use the 32-bit Oracle SQL*Loader" on page 625](#). Otherwise, run the IBM OpenPages with Watson Entity Move/Rename utility.

Avoid error 0509-036 when you use the 32-bit Oracle SQL*Loader

This task applies only to the Entity Move/Rename operation if you use the 32-bit SQL*Loader utility with Oracle databases in Linux environments. Skip this task if you are using the 64-bit SQL*Loader utility.

If you use the 32-bit SQL*Loader (**sqlldr**) utility, the following system error might be displayed:

```
exec(): 0509-036 Cannot load program sqlldr because of the following errors:  
      0509-026 System error: There is not enough memory available now.  
Failure while executing the Oracle SQL*Loader. Exit code is 255
```

If the 0509-036 system error is displayed, you can set the Loader Control environment variable by opening a shell window and running the following command:

```
export LDR_CNTRL=MAXDATA=0x80000000 at LARGE_PAGE_DATA=Y
```

Tip: If you are running the IBM OpenPages with Watson Entity Move/Rename utility as a scheduled **cron** job, make sure to set the Loader Control environment variable in the **cron** environment.

When finished, run the IBM OpenPages Entity Move/Rename utility. See “[Running the entity move/rename utility interactively](#)” on page 625 or “[Running the Entity Move/Rename utility as a scheduled task](#)” on page 576.

Running the entity move/rename utility interactively

Use the following steps to run the IBM OpenPages with Watson Entity Move/Rename utility interactively in an Oracle database environment.

Before you begin, make sure that you prepared the input file. See “[Prepare the input file for the Entity Move/Rename utility](#)” on page 574 for instructions.

Procedure

1. Move the input file into the utility installation directory, which is at:

```
OP_Home|aurora|bin|batch_entity_move_rename_relative
```

2. Validate that the **input_file** parameter in the `batch-entity-move-rename.ini` configuration file is correctly set to the input file name. For more information, see “[Configuring the Entity Move/Rename utility for an Oracle database](#)” on page 622.
3. From the location where the utility is installed, run the batch command file and review the output on the screen.

Windows

```
batch-entity-move-rename.cmd
```

Linux

```
batch-entity-move-rename.sh
```

4. Upon completion, review the following log files for any errors:

- `batch-entity-move-rename-load.log`
- `batch-entity-move-rename-proc.log`

If any errors are reported and you are unable to fix them, contact IBM OpenPages Support. Make sure you supply a copy of the screen that contains the error messages and all the log files that are generated by the tool.

Running the Entity Move/Rename utility as a scheduled task

You can set up a scheduled task to run the IBM OpenPages with Watson Entity Move/Rename utility.

Depending on your environment, you can run the `batch-entity-move-rename` batch command file by using any scheduling application. For example, in Windows, you might use the built-in Windows scheduler. In Linux, you might set up a **cron** job.

Important: If you are using a Db2 database in a Windows environment, you must run the batch command file within the **Db2 Command Line Processor**.

If the job fails, the batch command returns a non-zero exit code. You can redirect the console output to a log file. For example, in Windows:

```
batch-entity-move-rename.cmd >> batch-entity-move-rename.log
```

The following files are overwritten on each run:

- `batch-entity-move-rename-load.log`
- `batch-entity-move-rename-proc.log`

These files can be saved, either manually or through a script, if log archives are needed.

Impact of the Entity Move/Rename utility on the OpenPages application

The Entity Move/Rename utility works directly against the IBM OpenPages with Watson database repository. As a result, the Java based OpenPages application is unaware of the changes made to the entity hierarchy and folder structure.

As a result, internal application caches might become out of sync with the data in the repository and lead to discrepancies in the application user interface.

It is required that after you run the tool you restart application services, or run the tool when application services are stopped.

Also, ensure that the **OPBackup** command is not running during execution, and that all batch rename and move operations are completed before you run a backup.

Chapter 24. System Maintenance

You can perform system maintenance tasks such as changing the default port numbers, changing password references, and so on.

Application server restrictions

When you are performing system maintenance, be aware of the restrictions for IBM OpenPages with Watson application servers.

- Do not rename application servers. The OpenPages property files contain hard-coded references to the application servers.

Port assignments

Both dedicated ports and ports that are dynamically assigned for each installation are used for the IBM OpenPages with Watson installation. These default ports can be changed after installation.

Default ports

The following table lists the default ports.

Table 202. Default port assignments	
Description	Ports
OpenPages installation server	8443
OpenPages installation agent	8443
OpenPages database instance (Oracle)	1521
OpenPages database instance (IBM Db2)	50000
OpenPages application URL (HTTP)	10108
OpenPages application URL (HTTPS)	10111
IBM Cognos Analytics gateway (as configured for your web server)	80
IBM Cognos Analytics dispatcher URI	9300
Search server (used for indexing and searching OpenPages data)	8983
Search server (used to administer global search)	8985

Files containing port numbers

After installation, you can view the OpenPages application port assignments in the following file on each application server: <OP_HOME>/wlp-user/servers/<server_name>Server<#>/bootstrap.properties.

The following table lists property files on the OpenPages admin application server that contain port numbers for other components.

Table 203. Files that contain port numbers

Port	File name	Parameter Name
Application server ports	<OP_HOME>/wlp-usr/servers/ <server_name>Server<#/>/ bootstrap.properties	op.http.port op.https.port if you are using SSL
Oracle database instance port	<ORACLE_HOME>/NETWORK/ADMIN/ tnsnames.ora	N/A

IBM Cognos Analytics port numbers in settings

The table lists settings that contain port numbers for IBM Cognos Analytics.

Table 204. Settings that contain port numbers for IBM Cognos Analytics

Port	Setting
IBM Cognos Analytics server port	Platform > Reporting > Cognos Dispatcher Service URL For example: <code>http://<server_name>:<port>/ibmcognos/bi/v1/resp</code>
IBM Cognos Analytics SDK URL	Platform > Reporting > Cognos SDK URL For example: <code>http://<server_name>:<port>/p2pd/servlet/dispatch</code>
IBM Cognos Analytics logout URL	Platform > Reporting > Cognos Logout URL For example: <code>http://<server_name>:<port>/ibmcognos/bi/v1/resp?b_action=xts.run&m=portal/logoff.xts&h_CAM_action=logoff</code>

Dynamically assigned ports for application servers

Port numbers for IBM OpenPages with Watson servers are assigned during the installation process. The starting port number of an application server is defined in **OP Cluster Start Port** in the installation app. Dynamic ports are assigned starting from the **OP Cluster Start Port**.

For admin application servers, the following ports are used:

- **OP Cluster Start Port**
- **OP Cluster Start Port + 8**
- **OP Cluster Start Port + 11**
- **OP Cluster Start Port + 17**
- **OP Cluster Start Port + 18**

For non-admin application servers, the following ports are used:

- **OP Cluster Start Port**
- **OP Cluster Start Port + 8**
- **OP Cluster Start Port + 11**

If an application server has more than one vertical cluster member, two more ports are used for each of them. The ports are incremented by 20 for each vertical cluster member. For example, if an application server has two cluster members, that is **OP Vertical Cluster Number** = 2, the additional ports are:

- **OP Cluster Start Port** + 20 + 8
- **OP Cluster Start Port** + 20 + 11

The following list shows some examples:

Admin application server

If **OP Cluster Start Port** = 10100 and **OP Vertical Cluster Number** = 1, the required ports are:

- 10100
- 10108
- 10111
- 10117
- 10118

Non-admin application server

If **OP Cluster Start Port** = 10120 and **OP Vertical Cluster Number** = 1, the required ports are:

- 10120
- 10128
- 10131

Non-admin application server with vertical cluster members

If **OP Cluster Start Port** = 10120 and **OP Vertical Cluster Number** = 3, the required ports are:

- 10120
- 10128
- 10131
- 10148
- 10151
- 10168
- 10171

Change default port numbers

You can change the default IBM OpenPages with Watson port numbers after installation.

Important: Only ports 80, 443, or an open port in the range 1024 - 65535 can be used as the IBM OpenPages with Watson application port number.

The OpenPages with Watson installer sets several default ports during installation, such as the ports for the OpenPages server.

After installing the application, you can change the OpenPages ports to different ports, if needed. For example, in the event of a port conflict, where another application is using these port ranges, you can change the OpenPages ports to avoid the conflict.

For a port conflict, change all of the OpenPages application server ports to a new range. Follow the instructions in the following section.

Important:

- Do not change the port number for the OpenPages with Watson administrative server.
- To modify port numbers on other application servers in a cluster, repeat the following tasks on each cluster member.

Checking port number availability

Before changing the port numbers, make sure that the new ports you are going to use are available.

To determine if another application is using a specific port, log on to the application server where you need to change the port. Open a command or shell window and execute the following command:

Windows

```
netstat -an | findstr <port number>
```

Linux

```
netstat -an | grep <port_number>
```

Changing OpenPages with Watson application ports

Because the IBM OpenPages with Watson application on IBM WebSphere Liberty uses port ranges, if you need to change one of the OpenPages environment port numbers, you should change all of the OpenPages application server ports to a new range.

By default, the OpenPages with Watson application on WebSphere Liberty uses the port range 10101-10120.

Updating the port numbers in WebSphere

Use the following steps to change the default port numbers of an IBM OpenPages with Watson application server.

Procedure

1. Log on to the application server.
2. Stop the application servers.
For more information, see “[Stopping application servers](#)” on page 711.
3. Open the following file in a text editor: `<OP_HOME>/wlp/usr/servers/<server_name>Server<#>/bootstrap.properties`
Where `<server_name>` is the name of the application server.
4. Update the application port number.
 - If you are using TLS, update the `op.https.port` value.
 - If you are not using TLS, update the `op.http.port` value.
5. Save your changes.
6. Repeat these steps on each horizontal application server.
7. Restart the application servers.
For more information, see “[Starting application servers](#)” on page 709.

What to do next

If you changed the OpenPages application port or the secure application port, you must manually change the port values in the following properties files for the OpenPages application server for which you changed the ports:

- `<OP_HOME>/aurora/conf/aurora.properties`
- `Server<#>-sosa.properties`
- `Server<#>-server.properties`

Updating the Java Messaging ports on the OpenPages with Watson server

You can change the ports that are used by the Java Messaging Service.

About this task

WebSphere Liberty uses the Java Message Service (JMS) to enable Java clients and applications to create, send, receive, and read asynchronous requests.

Procedure

1. Log on to the application server.
2. Stop the application servers.
For more information, see [“Stopping application servers” on page 711](#).
3. Open the following file in a text editor: <OP_HOME>/wlp-usr/servers/<server_name>Server<#/>/bootstrap.properties
Where <server_name> is the name of the application server.
4. Update the application port number.
 - If you are using TLS, update the op.jmss.port value.
 - If you are not using TLS, update the op.jms.port value.
5. Save your changes.
6. Repeat these steps on each horizontal application server.
7. Restart the application servers.
For more information, see [“Starting application servers” on page 709](#).

Updating the application port values in the server and tools-client properties files

If you changed the IBM OpenPages with Watson OpenPages application port (10108 or 10111, for example), you must manually change the port values in the server and tools client properties files.

Procedure

1. Log on to each IBM OpenPages with Watson application server as a user with administrative privileges.
2. On Windows computers, start a Command Prompt window with the **Run as administrator** option. On Linux computers, open a shell.
3. Update the server properties file:
 - a) Go to the <OP_HOME>/aurora/conf directory and open the Server<#/>-server.properties file in a text editor.
 - b) Edit the following line to update the port number.

```
webclient.http.server.port=<port>
```
4. Save and close the file.
5. Go to the <OP_HOME>/bin directory.
6. Open the openpages-tools-client.properties file in a text editor.
7. If you changed the application port, update the rest.url.path property with the new port number.
For more information, see [“Tools properties and parameters” on page 934](#).

For example:

```
rest.url.path=https\://localhost\:10111/grc/api
```

8. Save and close the file.

9. Restart all OpenPages application servers.

For more information, see [Chapter 25, “Starting and stopping servers,” on page 709](#).

Updating port values in the aurora.properties file

You can update port values in the aurora.properties file.

Procedure

1. Log on to the IBM OpenPages with Watson admin server associated with the application server for which you changed ports as a user with administrator privileges.
2. On Windows computers, start a Command Prompt window with the **Run as administrator** option. On Linux computers, open a shell.
3. Go to the <OP_HOME>/aurora/conf directory where <OP_HOME> represents the installation location of the OpenPages application.
4. Locate the aurora.properties file in the conf directory and open the file in a text editor.
5. If you changed the OpenPages application port number (10108 or 10111 by default), update the port in the following property:

```
application.url.path=
```

Note: In a load balanced environment, the application.url.path value is the fully qualified domain name of the load balancer and its port number.

Updating port values in the database

If you updated any of the default IBM OpenPages with Watson ports, you must update the port value(s) in the REGISTRY_ENTRIES table in the IBM OpenPages database as follows.

Procedure

1. Log on to a machine with an SQL tool and access to the database server.
2. Run the following SQL commands to update the port number in the REGISTRY_ENTRIES table:

```
update registryentries set value='<new_port_number>'  
where path='/OpenPages/Platform/Reporting Schema/Object URL Generator/Port';  
commit;
```

where <new_port_number> is the new OpenPages application server port number.

3. When the commands are complete, log out of SQL*Plus.

Updating port values on the reporting server

If you changed the IBM OpenPages with Watson application port number, you must update the associated CommandCenter instance with the new port number.

Procedure

1. Log on to the reporting server as a user with administrator privileges.
2. Open an Linux shell and navigate to the <Cognos_Home>/configuration directory where <Cognos_Home> represents the installation location of the Cognos application.
3. Locate the OpenPagesSecurityProvider_OpenPagesSecurityRealm.properties file and make a backup copy of the file.
4. Open the OpenPagesSecurityProvider_OpenPagesSecurityRealm.properties file in a text editor of your choice and do the following:
 - a) Replace the existing OpenPages with Watson application port number (10108) update the following property with the new OpenPages application port number:

```
openpages.application.url=
```

- b) Save and close the file.

Updating URL host pointers for reports

After you migrate, change port settings in a production environment, or if you want to refresh a test environment from a production database, you might need to update the URL host pointers on the application server so that links in reports work properly.

You need to update the URL host pointers if the host, port, or protocol of the application server has changed. Check the **Object URL Generator** setting to verify that the host, port, and protocol are correct. If the port, host, and protocol are correct, you do not need to do this task.

You can update links in reports by modifying URL host pointer settings, and then propagating these reporting schema changes to the application server.

To update the reporting schema, you can do either of the following:

- Run an SQL script that incrementally updates the reporting schema with the changes (recommended).
Note: For SQL tool information, see the topic "Database tool information" in the *IBM OpenPages with Watson Administrator's Guide*.
- Use the IBM OpenPages with Watson application user interface to re-create the entire reporting schema.

Procedure

1. Start the IBM OpenPages with Watson services on the admin application server.
2. Log on to the OpenPages with Watson application user interface as a user with administrator privileges.
3. Click  > **System Configuration** > **Settings**.
To access settings, you must have the **Settings** application permission set on your account.
4. Change the **Object URL Generator** settings.
 - a) Expand **Platform** > **Reporting Schema** > **Object URL Generator**.
 - b) Update the **Object URL Generator** settings, as required, to point to the application server (such as a test application server). Make sure to click **Save** after you modify each setting.

Table 205. Object URL Generator settings

Setting Name	Description
Host	The changed name of the application server. Example : test-eng1
Port	The changed port number of the application server. Example : 10108
Protocol	The changed protocol for accessing the application server. Valid values are either http or https.

5. To update the changed URL setting on the application server, update the reporting schema using one of the following methods:
 - Method 1: Run the following SQL script to incrementally update the reporting schema (recommended):

- a. From a computer with a SQL tool and access to the database server, log on to SQL as the OpenPages database user (for example, openpage).
- b. Run the following SQL statements to update the reporting schema:

```
begin
OP_RPS_MGR.SET_DETAIL_PAGE_URL_IN_RPS_RT;
end;
/
```

- Method 2: Re-create the entire reporting schema by using the application user interface. For more information, see "Creating or re-creating the reporting schema" in the *IBM OpenPages with Watson Administrator's Guide*.

Auditing configuration changes

IBM OpenPages with Watson provides you with the capability of tracking configuration changes made to your system through the Configuration Audit Report.

Accessing the Configuration Audit report

To view and generate the Configuration Audit Report, you must have the reporting schema and framework enabled and configured on your system.

Procedure

1. Click  > **Analytics**.
2. From the IBM Cognos Analytics with Watson menu, click **Content**.
3. On the **Team content** tab, click **OpenPages Platform Reports > Audit Reports > Configuration**.
4. Click **Configuration Audit** to run the report.
5. On the **Configuration Audit Report** page, specify the date range for the reporting data as follows:
 - a) Type a start date or click the calendar arrow and select a start date.
 - b) Type an end date or click the calendar arrow and select an end date.
 - c) Click **Finish** to generate the report.

The Configuration Audit report

The Configuration Audit report tracks any metadata changes made to field groups, object types, application text, object text, profiles, settings, and views and dashboards.

- Field Groups - such as modifications made to object field definitions and enumerated string values.
- Object Types - such as the inclusion of Field Groups and changes in parent and/or child object relationship rules (for example, cardinality setting changes or enabling/ disabling object type relationships).
- Application Text or Object Text - such as translation changes to locale-specific display labels for object types, object fields, and enumerated string values. You can enable or disable the auditing of translated text. By default, auditing is enabled.
- Profiles - such as modifying object views and showing or hiding object types and fields.
- Registry settings.
- Views.
- Dashboards.

[Table 206 on page 635](#) describes the various audited configuration changes contained in the report under the following column headings:

Table 206. Audit Configuration column headings

This report column...	Contains this type of data...
Object	The type of object that was modified.
Category	A category or classification under the object type.
Action Type	The type of action performed on the object.
Action Date	The date the action was performed.
Created by	The name of the user who performed the action.
Old Value	The value before it was modified.
New Value	The value after it was modified.

Changing the password of the WebSphere Liberty keystore

You can change the password of the IBM WebSphere Liberty keystore.

Procedure

1. Log on to the OpenPages admin application server.
2. Open a command or shell window.
3. Run the following command:

```
keytool -storepasswd -keystore <OP_HOME>/wlp/usr/servers/<server_name>Server<#/>/resources/security/key.p12 -storetype PKCS12 -storepass <current_password>
```

Replace *<current_password>* with the current password of the keystore. The initial password of the keystore is the same as the OpenPagesAdministrator password that you set when you installed OpenPages.

4. Follow the prompts to set the new password.
5. Encrypt the password by running the following command:

```
<WLP_HOME>/bin/securityUtility.sh|.bat encode --encoding=aes <new_password>
```

Replace *<new_password>* with the password that you created in step 4.

The script returns the encrypted password.

6. Update the *bootstrap.properties* file with the new encrypted password.
 - a) Open the following file in a text editor: *<OP_HOME>/wlp/usr/servers/<server_name>Server<#/>/bootstrap.properties*
 - b) Update the value of the *keystore.password* parameter with the encrypted password from step 5.
 - c) Save and close the file.
7. Restart all application services.
For more information, see “[Starting application servers](#)” on page 709.
8. Repeat these steps on each horizontal cluster application server.

Changing the keystore that is used by WebSphere Liberty

When you install IBM OpenPages with Watson, the installation process configures a keystore for IBM WebSphere Liberty. If you have an existing keystore or if you want to use an alternate keystore, you can change the keystore that is used by WebSphere Liberty. This task is optional.

Procedure

1. Log on to the application server.
2. Encrypt the password of the keystore that you want to use for WebSphere Liberty.

Run the following command:

```
<WLP_HOME>/bin/securityUtility.sh|.bat encode --encoding=aes <keystore_password>
```

Replace *<keystore_password>* with the password of the keystore.

The script returns the encrypted password.

3. Edit the following file:

```
<OP_HOME>/wlp-usr/servers/<server_name>/configDropins/overrides/op-apps.xml
```

4. Update the following line to point to the keystore that you want to use.

```
<keyStore id="defaultKeyStore" location="<keystore_file>" password="<encrypted_password>" />
```

Replace *<keystore_file>* with the path and filename of the keystore. Replace *<encrypted_password>* with the encrypted password from step 2.

For example:

```
<keyStore id="MyKeyStore" location="/home/opuser/OP/OpenPages/wlp-usr/servers/opappServer1/resources/security/my_keystore.p12" password="<encrypted_password>" />
```

5. Restart all application services.

For more information, see [“Starting application servers” on page 709](#).

6. Repeat these steps on each horizontal cluster application server.

Changing the keystore that is used by Db2

When you install IBM OpenPages with Watson, the installation process configures a keystore for IBM WebSphere Liberty. By default, the Liberty keystore is also used for Db2. If you have an existing keystore or if you want to use an alternate keystore, you can change the keystore that is used by Db2. This task is optional.

Procedure

1. Log on to the application server.
2. Locate the keystore that you want to use for Db2 and copy it to the following directory on the application server: *<OP_HOME>/wlp-usr/servers/<server_name>Server<#>/resources/security/*
3. Copy the *<OP_HOME>/wlp-usr/servers/<server_name>Server<#>/op-db2.xml* file to the following directory: *<OP_HOME>/wlp-usr/servers/<server_name>Server<#>/configDropins/overrides/*.
Do not modify or delete the *<OP_HOME>/wlp-usr/servers/<server_name>Server<#>/op-db2.xml* file.
4. Open the following file in a text editor: *<OP_HOME>/wlp-usr/servers/<server_name>Server<#>/configDropins/overrides/op-db2.xml*
5. Locate the following line:

```
<properties.db2.jcc databaseName="op_db_name" portNumber="op_db.port"  
serverName="op_db.host" user="op_jdbc_user" password="op_jdbc_password"  
enableExtendedDescribe="2" />
```

6. Add the following attributes to the properties.db2.jcc element:

```
sslTrustStoreLocation="db_keystore_file" sslTrustStorePassword="db_keystore_password"  
sslTrustStoreType="PKCS12"
```

Replace *db_keystore_file* with the path and filename of the keystore. Replace *db_keystore_password* with the encrypted password of the keystore.

For example:

```
<properties.db2.jcc databaseName="OPX" portNumber="50001" serverName="db.host.com" user="op"  
password="password" enableExtendedDescribe="2"  
sslTrustStoreLocation="/home/opuser/OP/OpenPages/wlp/usr/servers/opappServer1/  
resources/security/db.p12" sslTrustStorePassword="password" sslTrustStoreType="PKCS12" />
```

7. Restart all application services.

For more information, see “[Starting application servers](#)” on page 709.

8. Repeat these steps on each horizontal cluster application server.

Changing the OPSystem password

You can change the password of the OPSystem account. OPSystem is a default service user account that is required by internal system actions.

Procedure

1. Start all services.
2. Open a command or shell window on the application server.
3. Navigate to the *<OP_HOME>/bin* directory.

For Microsoft Windows operating systems, the default installation directory of OpenPages with Watson is C:\OpenPages.

For Linux operating systems, the default installation directory of OpenPages with Watson is /opt/OpenPages.

Tip: You can also run the chng-sys-pswd tool from a remote system, such as your laptop. For more information, see “[Installing tools and utilities \(IBM OpenPages with Watson\)](#)” on page 692

4. Run one of the following commands to open the chng-sys-pswd tool:

Windows

chng-sys-pswd.bat

Linux

chng-sys-pswd.sh

You are prompted for the old OPSystem password, and then the new password.

5. Follow the on-screen prompts.
6. When directed, stop all services.
7. Restart all services to enable the new password.

Changing database password references

If the password of the OpenPages database changes, you need to update password references with the new password.

Before you begin

Before you change password references for data sources in IBM OpenPages with Watson, make sure that you have the following:

- Administrative access to the following machines and application:
 - OpenPages application server
 - IBM Cognos Analytics server
 - IBM Cognos Analytics application
- The current and new password for the following database users:
 - OpenPages database user

About this task

To change database password references, you must do the following tasks:

- [“Change database password references on the OpenPages with Watson application server” on page 638](#)
- [“Modifying the OpenPages database password in Cognos ” on page 639](#)
- [“Modifying database passwords in the backup-restore environment files” on page 640](#)

If you need information about encrypting database passwords in the backup and restore utility environment files, see [“Encrypting database passwords in the backup-restore utility environment files” on page 581](#).

- If you use global search, update the login information for the search server. See [“Changing the login information for the search server” on page 520](#)

Change database password references on the OpenPages with Watson application server

The process for changing the database password on the IBM OpenPages with Watson application server requires two tasks.

[“Modifying the JDBC data source password” on page 638](#)

[“Updating the application server database password in the aurora.properties file” on page 639](#)

Important: Make a backup copy of each file before modifying it.

Modifying the JDBC data source password

If the JDBC data source password changes, you need to update the `bootstrap.properties` file on each application server.

Procedure

1. Log on to the OpenPages application server.
2. Open a command or shell window.
3. Encrypt the password by running the following command:

```
<WLP_HOME>/bin/securityUtility.sh|.bat encode --encoding=aes <new_jdbc_password>
```

Replace `<new_jdbc_password>` with the database password.

The script returns the encrypted password. Copy the password.

4. Update the `bootstrap.properties` file with the new encrypted password.

- a) Open the following file in a text editor: <OP_HOME>/wlp-usr/servers/<server_name>Server<#/>/bootstrap.properties
 - b) Update the value of the op.jdbc.password parameter with the encrypted password from step 3.
 - c) Save and close the file.
5. Restart all application services.
For more information, see “[Starting application servers](#)” on page 709.
6. Repeat these steps on each horizontal cluster application server.

Updating the application server database password in the aurora.properties file

To change the database password on the IBM OpenPages with Watson application servers, one task that you must do is to edit the aurora.properties file.

Procedure

1. Open a command or shell window and navigate to the <OP_HOME>/aurora/conf directory.

Table 207. Installation location of the OpenPages with Watson application

Operating system	Installation location
Windows	For example, <OP_HOME> C:\IBM\OpenPages
Linux	For example, <OP_HOME> /opt/IBM/OpenPages

2. Locate the aurora.properties file in the conf directory and do the following steps:
 - a) Make a backup copy of the file before modifying it.
 - b) Open the file in a text editor of your choice.
 - c) Search the file for the string database.PASSWORD.
 - d) Change the value following the equal sign to the new password.
 - e) Save your changes and exit the editor.

Note: The password becomes encrypted when the services are restarted.

3. Repeat these steps on each application server.

Modifying the OpenPages database password in Cognos

If you change the IBM OpenPages with Watson database password, you must update the OpenPages DataSource in IBM Cognos Analytics. If you have an Oracle database environment, you must also update the Oracle Native Driver.

Procedure

1. Ensure that all application servers and reporting servers are running.
2. Open a browser window and log on to the OpenPages with Watson application user interface as a user with administrative permissions.
3. Click  > **Analytics**.
4. Click **Manage > Administration Console** to launch the **IBM Cognos Administration** page.
5. Click the **Configuration** tab.
6. Click the link for the **OpenPages DataSource**, and then click **OpenPages DataSource**.
The **Directory > Cognos > OpenPages DataSource > OpenPages DataSource** page is displayed.
7. Under the **Actions** column, click the **Set properties - OpenPages DataSource** icon .
8. Click the **Signon** tab.

9. Click the **Edit the signon** link.
10. Type the password of the OpenPages database, and then click **OK**.
11. If you use Oracle, do the following additional steps:
 - a) Return to the **Directory > Cognos** page.
 - b) Click the link for the **Oracle Native Driver**, and then click **Oracle Native Driver**.
The **Directory > Cognos > Oracle Native Driver > Oracle Native Driver** page is displayed.
 - c) Click the **Signon** tab.
 - d) Click the **Edit the signon** link.
 - e) Type the password of the OpenPages database, and then click **OK**.
12. Log out of OpenPages.
13. Restart all OpenPages application servers.
14. Log on to OpenPages and open a report to test Cognos.

Modifying database passwords in the backup-restore environment files

If you change the IBM OpenPages database password, you need to update the environment files that are used by the backup and restore utilities.

Procedure

1. Repeat these steps on each application server.
2. Open a command or shell window as an administrator.
3. Go to the `<OP_HOME>/aurora/bin` directory and locate the `op-backup-restore.env` file.
4. Make a backup copy of the `op-backup-restore.env` file.
5. Open the `op-backup-restore.env` file in a text editor.
6. Update the following passwords:

Db2

- `DB_OP_PWD`: Type the password of the schema owner for the OpenPages database.

Oracle

- `DB_SYSTEM_PWD`: Type the password of the SYSTEM user for the OpenPages database.
- `DB_SYS_PWD`: Type the password of the DBA user for the OpenPages database.
- `DB_OP_PWD`: Type the password of the schema owner for the OpenPages database.

7. If you're using Oracle, do the following steps:
 - a) Go to the `<CC_HOME>/tools/bin` directory and locate the `op-cc-backup-restore.env` file.
 - b) Make a backup copy of the `op-cc-backup-restore.env` file.
 - c) Open the `op-cc-backup-restore.env` file in a text editor.
 - d) Update the `DB_CC_PWD` password.

Type the password of the schema owner for the Cognos database.

Note: If you use the same database for OpenPages and the Cognos content store, enter the passwords for the OpenPages database DBA and schema owner.

8. Re-encrypt the passwords in the `op-backup-restore.env` and `op-cc-backup-restore.env` files.
See “[Encrypting database passwords in the backup-restore utility environment files](#)” on page 581.
9. Repeat these steps on each application server.

Updating the Oracle Enterprise Manager tool

If either the static IP address of the database server changes or the database hostname changes, then the web-based Oracle Enterprise Manager tool (https://<server_name>:<port>/em), which is used for managing the Oracle database, will no longer function properly and requires reconfiguration.

Note: The Oracle database server requires a static IP address.

Resolving configuration changes in the Oracle EM tool

To resolve configuration changes so the Oracle Enterprise Manager Database Control tool functions properly, you must first deconfigure and then reconfigure the tool.

Procedure

1. Open a command or shell window.
2. Go to the `<ORACLE_HOME>/bin` directory.
3. Type the following command to deconfigure the Oracle Enterprise Manager tool:

```
emca -deconfig dbcontrol db -repos drop
```

4. Type the following command to reconfigure the Oracle Enterprise Manager tool:

```
emca -config dbcontrol db -repos create
```

Changing database name references

If the database name (IBM Db2) or identifier (Oracle) changes, you need to update references to the database.

For example, if you have upgraded from an old database server to a new one, migrated from a non-RAC to a RAC environment, or are moving from a shared database environment to a stand-alone environment, then you must change several references on the IBM OpenPages with Watson application and reporting servers to point to the new database instance.

Note:

If you changed the database server hostname, see the following topics:

- If you are using IBM Db2, see [How to Change the Hostname of an IBM DB2 Database Server for OpenPages](#).
- If you are using Oracle, see [How to Change the Hostname of an Oracle Database Server for OpenPages](#).

To change database references, you must take the following actions:

- If you are using IBM Db2, re-create the catalog entry for the OpenPages database, and then test the connection. You can see examples of the syntax in the following technote: [How to Change the Hostname of an IBM DB2 Database Server for OpenPages](#).
- If you are using Oracle, see “[Testing the connection to the OpenPages database from the Oracle database client](#)” on page 642
- “[Modifying the data source connection URL](#)” on page 642
- “[Modify database references in the application configuration files](#)” on page 643
- “[Modify database connection references for the reporting server](#)” on page 644

Before you begin

Make sure that you have the following information:

- Administrative access to the following machines and application:
 - OpenPages application server

- OpenPages Cognos server
- IBM Cognos Analytics application
- OpenPages system account user and password
- For Oracle database environments, the Oracle System Identifier (SID) of the new database instance.
- For IBM Db2 database environments, the database name.

Testing the connection to the OpenPages database from the Oracle database client

Test whether the SQL*Net connect string can connect to the IBM OpenPages with Watson database on the Oracle database server from the Oracle database client.

Procedure

1. Copy the file <ORACLE_HOME>/network/admin/tnsnames.ora from the Oracle database server operating system to the <ORACLE_HOME>/network/admin Oracle database client directory on the application server or reporting server.
Ensure that the OpenPages installation user has read, write and execute permissions on the tnsnames.ora file in the Oracle database client operating system.
2. Log on to the application server or reporting server as an OpenPages installation user.
3. Edit the file <ORACLE_HOME>/network/admin/tnsnames.ora, and update the Host value to the hostname or IP address of the Oracle database server.
4. To test the connection to the OpenPages database on the database server, type the following command:

```
sqlplus <username>/\"<password>\\"@<service_name>
```

For example, sqlplus system/\"password\\"@op

The system connects you to an Oracle database instance.

5. To exit SQL*Plus, type exit.

Modifying the data source connection URL

You can modify the JDBC data source in IBM WebSphere Liberty for the application server.

Procedure

1. Log on to the OpenPages application server.
2. Open the following file in a text editor: <OP_HOME>/wlp/usr/servers/<server_name>Server<#/>/bootstrap.properties
3. Update the properties.

Db2

Set op.jdbc.host to the hostname of the database server.

Set op.db2.portNumber to the database port number.

Set op.db2.databaseName to the name of the Db2 database.

Oracle

Set op.jdbc.host to the hostname of the database server.

Set op.ora.portNumber to the database port number.

Set op.ora.databaseName to the Oracle System Identifier.

4. Save the file.
5. Restart all application services.

For more information, see “[Starting application servers](#)” on page 709.

6. Repeat these steps on each horizontal cluster application server.

Modify database references in the application configuration files

Use the following instructions to update database references in the `aurora.properties` file. If you are using Oracle, you also need to update the `op-backup-restore.env` file.

Modify the database reference in the `aurora.properties` file

You can update the database references in the `aurora.properties` file.

Procedure

1. Open a command or shell window and go to the `<OP_HOME>/aurora/conf` directory.
2. Locate the `aurora.properties` file in the `conf` directory and do the following tasks:
 - a) Make a backup copy of the file before you modify it.
 - b) Open the file in a text editor of your choice.
 - c) Search the file for the string ‘`database.URL`’.
 - d) Change the value that follows the equal sign to the new database connection URL.
 - For Oracle database environments, the URL format might look similar to the following example.

```
database.URL=jdbc\:oracle\:thin\:@//<host-name>\:<port>/<SID>
```

Where:

- `<host-name>` is the name of the database server, such as `eng11`.
 - `<port>` is the database port number, such as `1521`.
 - `<SID>` is the Oracle System Identifier, such as `OP`.
- For IBM Db2 environments, the URL format might look similar to the following example.

```
database.URL=jdbc\:db2\://<host-name>\:<port>/<db_name>
```

Where:

- `<host-name>` is the name of the database server, such as `eng11`.
- `<port>` is the database port number, such as `50000`.
- `<db-name>` is the name of the Db2 database, such as `OP`.

- e) Save your changes and exit the editor.
3. Repeat these steps on each application server.

What to do next

If you are using Oracle, update the `op-backup-restore.env` file. For more information, see “[Modify database references in the OpenPages backup and restore environment file \(Oracle only\)](#)” on page 643.

Modify database references in the OpenPages backup and restore environment file (Oracle only)

This task applies only to Oracle database environments. You must modify Oracle database references in the `op-backup-restore.env` file.

Procedure

1. Open a command or shell window and navigate to the `<OP_HOME>/aurora/bin` directory.

For information about <OP_HOME>, see “[Installation locations \(on prem\)](#)” on page 2.

2. Locate the op-backup-restore.env file in the bin directory and do the following:

- a) Make a backup copy of the file before modifying it.
- b) Open the file in a text editor of your choice.
- c) Search the file for the following strings:
 - DATABASE_URL=jdbc:oracle:thin:@//<host-name>:<port>/<SID>
 - DB_SID=<SID>
 - DB_ALIAS=<database_alias>

Where:

- <host-name> is the name of the database server, such as eng11.
- <port> is the database port number, such as 1521.
- <SID> is the system ID of the database, such as OP.
- <database_alias> is the alias of the database, such as OP.

- d) Change the value following the equal sign to the new database connection URL and SID.
- e) Save your changes and exit the editor.

3. Restart the OpenPages application servers.

4. Repeat these steps on each application server.

Modify database connection references for the reporting server

Use the following instructions to update database references in IBM Cognos Analytics. If you have an Oracle database environment, you must also update the op-cc-backup-restore.env file.

Once the values are updated, you need to restart all reporting servers.

Modifying database connection references in Cognos

You must change the database connection reference values in IBM Cognos Analytics for the OpenPages DataSource. If you have an Oracle database environment, you must also update the Oracle Native Driver.

Procedure

1. Ensure that both the IBM OpenPages with Watson and IBM Cognos servers are running.
2. Open a browser window and log on to the OpenPages with Watson application user interface as a user with administrative permissions.
3.  > **Analytics**
4. Click **Manage > Administration Console** to launch the **IBM Cognos Administration** page.
5. In the **IBM Cognos Administration** window, click the **Configuration** tab.
6. On the **Directory > Cognos** page, click the link for the **OpenPages DataSource**.
7. On the **Directory > Cognos > <data-source-name>** page, do the following:
 - a) Under the **Actions** column, click the **Set properties - OpenPages DataSource** icon .
 - b) On the **Set properties - OpenPages DataSource** page, click the **Connection** tab.
8. On the **Connection** tab, do the following:
 - a) Next to the **Connection String** box, click the pencil icon.
 - b) On the **OCI** tab, on the **Edit the connection string - Oracle** page, edit the SID value in the **SQL*Net connect string** field.
 - c) On the **JDBC** tab, edit the values in the **Server name**, **Port number**, and **Oracle Service ID** boxes.

9. For the Oracle Database environments, return to the **Directory > Cognos** page, and click the link for the **Oracle Native Driver** and repeat Steps 7-8 for the Oracle Native Driver.
10. Restart all administrative and managed servers.

Modifying database reference in the Cognos backup and restore environment file (Oracle only)

You must modify Oracle database references in the Cognos backup and restore environment file. This task applies only to Oracle database environments.

Procedure

1. Open a command or shell window and go to the `<CC_Home>|tools|bin` directory.
2. Locate the `op-cc-backup-restore.env` file in the `bin` directory and do the following tasks:
 - a) Make a backup copy of the file before you modify it.
 - b) Open the file in a text editor of your choice.
 - c) Search the file for the string `DB_ALIAS`.
 - d) Change the value that follows the equal sign to the new Cognos database alias. The format might look similar to the following example:

```
DB_ALIAS=<CommandCenter Database Alias>
```

Example

```
DB_ALIAS=OP
```

- e) Save your changes and exit the editor.
3. Restart the reporting server.
4. Repeat these steps on each reporting server (active and standby).

Modifying database connection references in Cognos Configuration

You can modify database connection references in IBM Cognos Configuration.

Procedure

1. Log on to the reporting server as a user with administrative privileges.

Note: For a Linux server, log on as a non-root user.

2. Start the IBM Cognos Configuration tool:

- a) Open a Command Prompt window (using the **Run as administrator** option), or a Linux shell and navigate to the `<COGNOS_HOME>/bin64` directory.
- b) Run one of the following commands to open the tool:

Windows:

```
cogconfig.bat
```

Linux:

```
./cogconfig.sh
```

3. In the **Explorer** pane, do the following steps:

- a) Expand **Data Access** (if not already expanded).
- b) Under **Content Manager**, click **Content store**.
4. In the properties pane, modify the values for the following properties:
 - a) Database server and port number (for example, eng11:1527).
 - b) User ID and password

- c) Service name (for example, OP).
5. When finished, exit from Cognos Configuration.
6. Restart the Cognos server to apply the changes.

For more information, see [“Starting and stopping the Cognos services” on page 717](#).

Storing passwords in a vault

You can use a vault to store the OpenPages database user password, the OPSystem user password, or both.

This topic applies to IBM OpenPages with Watson traditional on-premises and IBM OpenPages with Watson on Cloud.

Before you begin

- You need a [CyberArk vault](#).
- Request an SSL certificate from your CyberArk administrator. The certificate is required to authenticate the connection between OpenPages and CyberArk.
- In CyberArk, create an Application for OpenPages. For more information, see the [CyberArk documentation](#).
- In CyberArk, add one or both of the following user accounts to the vault. Put the accounts into the same safe within the vault.
 - The OpenPages database user, for example openpage
 - The OPSystem user

About this task

When OpenPages needs a password, it retrieves it from the vault. When you need to change the password, you update it in the vault.

Procedure

1. Set up the SSL certificate keystore with the client certificate and server certificates:
 - a) Add the client certificate to the keystore. If the client certificate is in .crt or .pem format, convert it:

In this example, the client certificate is cyberark-client.p12 and the keystore is cyberark-ss18.p12.

```
keytool8 -importkeystore -srckeystore cyberark-client.p12 -srcstoretype pkcs12  
-destkeystore cyberark-ss18.p12 -deststoretype pkcs12
```
 - b) Add any server certificates to the same keystore by running the following command:

In this example, the server certificate is cpd-cyberark1-chain.pem.

```
keytool8 -importcert -file cpd-cyberark1-chain.pem -alias cpd-cyberark -keystore cyberark-ss18.p12 -storetype pkcs12
```
 - c) Copy the keystore file to the following directory on each application server: <OP_HOME>/aurora/conf/.

For example: <OP_HOME>/aurora/conf/cyberark-ss18.p12
2. Configure the vault properties.
 - a) Log in to the application server and go to the <OP_HOME>/aurora/conf/ directory.
 - b) Create a file called **vault.properties**.
 - c) Copy the following text into the file:

```

implementation=CyberArk
cyberark.safe=
cyberark.account=
cyberark.db.user=
cyberark.db.object=
cyberark.opsystem.object=
cyberark.keystore.file=
cyberark.keystore.pass=
cyberark.url=
cyberark.ssl.disable.hostname.verification=true|false
cyberark.keystore.type=pkcs12
cyberark.db.folder=
cyberark.opsystem.folder=

```

d) Configure the following properties in the file:

Table 208. Vault properties

Property	Description
cyberark.safe	Type the name of the vault. For example: OpenPagesSafe
cyberark.account	Type the unique ID of the application (App ID) that you created in CyberArk for OpenPages.
cyberark.db.user cyberark.db.object	If you are storing the OpenPages database user password in the vault, complete these fields. <ul style="list-style-type: none"> • cyberark.db.user: Type the username of the OpenPages database user. The name must match the name in the vault. • cyberark.db.object: Type the account name (unique ID) of the object in your vault that stores the database password. For example: cyberark.db.user=openpage cyberark.db.object=Database-Oracle-openpage
cyberark.opsystem.object	If you are storing the OPSSystem password in the vault, type the account name (unique ID) of the object in your vault that stores the OPSSystem password.
cyberark.keystore.file	Type the absolute path to the keystore that contains the CyberArk server certificates. For example: /home/opuser/OP/OpenPages/aurora/conf/cyberark-ssl8.p12 An absolute file path is required because the same properties file will be used by multiple components that will have different relative path locations.
cyberark.keystore.pass	Type the password of your client certificate keystore.

Table 208. Vault properties (continued)

Property	Description
cyberark.url	Type the HTTPS URL for CyberArk. For example: <code>https://myserver-cyberark.com</code>
cyberark.ssl.disable.hostname.verification	Set to <code>false</code> (default) unless the SSL server certificate and the hostname of the CyberArk environment are not the same. You might encounter this situation in non-production environments that use self-signed certificates.
cyberark.keystore.type	This property must be set to <code>pkcs12</code> .
cyberark.db.folder	Optional Specifies the CyberArk folder in the safe under which <code>cyberark.db.object</code> is located. Leave blank if you don't need this property.
cyberark.opsystem.folder	Optional Specifies the CyberArk folder in the safe under which <code>cyberark.opsystem.object</code> is located. Leave blank if you don't need this property.

3. If you're storing the database password in the vault, update the Liberty database data source files (`op-ora.xml` or `op-db2.xml`) on each application server.
 - a) Go to the `<OP-HOME>/wlp-usr/servers/<server-name>-OPNode1Server1` directory.
 - b) Open the `op-ora.xml` or `op-db2.xml` file.
 - c) Add the following `jaasContextEntry` elements:

```

<jaasLoginContextEntry id="vaultJAASLoginEntry" name="vaultJAASLoginEntry"
  loginModuleRef="vaultLoginModule" />
  <jaasLoginModule id="vaultLoginModule"
    className="com.ibm.openpages.vault.jaas.VaultDBLoginModule" controlFlag="REQUIRED"
    libraryRef="vaultJaasLibrary">
    <options VaultPropertiesPath="${openpages.home}/aurora/conf/vault.properties"/>
  </jaasLoginModule>

  <library id="vaultJaasLibrary">
    <fileset dir="${openpages.home}/aurora/lib" includes="com.ibm.openpages.vault.jar"/>
    <fileset dir="${openpages.home}/aurora/lib"
      includes="com.ibm.openpages.vault.jaas.jar"/>
      <fileset dir="${openpages.home}/aurora/lib" includes="httpclient-*.*jar"/>
      <fileset dir="${openpages.home}/aurora/lib" includes="httpcore-*.*jar"/>
      <fileset dir="${openpages.home}/aurora/lib" includes="commons-logging-*.*jar"/>
      <fileset dir="${openpages.home}/aurora/lib" includes="jackson-annotations-*.*jar"/>
      <fileset dir="${openpages.home}/aurora/lib" includes="jackson-core-*.*jar"/>
      <fileset dir="${openpages.home}/aurora/lib" includes="jackson-databind-*.*jar"/>
      <fileset dir="${openpages.home}/aurora/lib" includes="bcprov-jdk15to18-*.*jar"/>
      <fileset dir="${openpages.home}/aurora/lib" includes="aurora-tools.jar"/>
  </library>

```

- d) Update both of the `<dataSource...>` elements in the file to add the following attribute:

```
jaasLoginContextEntryRef="vaultJAASLoginEntry"
```

- e) Remove the `op.jdbc.password` attribute from the nested properties of each of the `dataSource` elements.
- f) Open the `<OP-HOME>/wlp-usr/servers/<server-name>-OPNode1Server1/bootstrap.properties` file and remove the `op.jdbc.password` property.

- g) Repeat these steps on each application server.
4. If you're storing the database password in the vault and you are using an Oracle database, do the following steps:
- a) Edit the `/home/opuser/OP/OpenPages/aurora/bin/op-backup-restore.env` file.
 - b) Set the following property:
- ```
VAULT_IMPLEMENTATION=CyberArk
```
- c) Comment out or remove the `DB_OP_PWD` property.
  - d) Repeat these steps on each application server.
5. If you're storing the database password in the vault and you use Global Search, do the following steps:
- a) If the global search server is on a different host than the application server, copy the `vault.properties` file and the certificate `.p12` file to the search server.
  - b) Edit the `/home/opuser/OP/OPSearch/opsearchtools/openpages_search.properties` file.
  - c) Change the line `OPSearchTool.DatabaseVaultProperties=` to the absolute path of the `vault.properties` file on the search server.
  - d) Comment out the `OPSearchTool.DatabasePassword` property.
  - e) Restart the search server.
6. If you're storing the OPSystem password in the vault, do the following steps:
- a) Open the `aurora.properties` file.
  - b) Remove or comment out the following property:
- ```
security.system.password
```
- c) Repeat these steps on each application server.
7. Restart all application servers.
8. If you use Global Search, restart the search server.

What to do next

When you need to change the database password, update it in the vault. Next, update IBM Cognos Analytics with the new password. See “[Modifying the OpenPages database password in Cognos](#)” on page 639.

Note: If you're using Global Search, do not use the `opsearchtool.sh` script to change the database password for the search server.

When you need to change the OPSystem password, update it in the vault, and then run the `chng-sys-pswd` utility. See “[Changing the OPSystem password](#)” on page 637.

TLS for OpenPages with Watson environments

You can configure OpenPages with Watson to use Transport Layer Security (TLS).

TLS establishes an encrypted link between the application server and web browsers, and between the application server and the other servers with which it communicates, such as the database server. The encryption ensures that all data that is passed between them remains private.

By default, OpenPages with Watson uses the TLSv1.2 protocol.

You can change the list of cipher suites that are enabled in IBM WebSphere Liberty. For more information, see the [Liberty documentation](#).

For information about the cipher suites that are supported by Java, see the [Java documentation](#).

Accessing the OpenPages with Watson application using TLS

You can access the IBM OpenPages with Watson application using a secure TLS connection. This procedure assumes that the default settings were not changed during installation.

Note: You must have an TLS digital certificate to use TLS with IBM OpenPages with Watson.

Open a browser window, and enter the following URL:

```
https://<server_name>:<tls_port>/openpages
```

Where <server_name> is the name of the server that hosts the OpenPages with Watson application, and <tls_port> is the TLS port number of the server.

For example:

```
https://server01.com:10111/openpages
```

Verifying TLS ports on application servers

Verify application ports in the <OP_HOME>/wlpusr/servers/<server_name>Server<#>/bootstrap.properties file on each horizontal cluster member.

Procedure

1. Log on to the application server.
2. Open the following file in a text editor: <OP_HOME>/wlpusr/servers/<server_name>Server<#>/bootstrap.properties
Where <server_name> is the name of the application server.
3. Check that the HTTPS port is correct.

For example:

```
op.https.port=10111
```

4. If any HTTPS ports are missing, add them.
5. Save your changes.
6. Repeat these steps on each horizontal application server.
7. Restart the application servers.

For more information, see [“Starting application servers” on page 709](#).

Generating a Certificate Signing Request file

If you require an authorized certificate from a third-party certificate authority (CA), you can use Keytool to generate the required certificate signing request (CSR). Keytool is provided with IBM SDK, Java Technology Edition.

About this task

Use the keytool -certreq command to generate a CSR file. Contact your CA for information about their requirements for the CSR file. For information about -certreq, see [-certreq](#) in the IBM SDK, Java Technology Edition documentation.

The default location of the keystore on application servers is <OP_HOME>/wlpusr/servers/<server_name>Server<#>/resources/security/key.p12

Importing signed CA certificates

You must install a root certificate and a server certificate from a trusted third-party certificate authority (CA) on each application server. You might also need to install an intermediate certificate on each

application server. You can use Keytool to import these certificates on the cluster administrator server and all cluster member systems. Keytool is provided with IBM SDK, Java Technology Edition.

Do this step after you receive the certificate from the Certificate Authority (CA). Use an ASCII PEM encoded certificate.

Use the `keytool -importcert` command to import the certificate. For more information, see [Importing a Certificate Reply and -importcert](#).

The default location of the keystore on application servers is `<OP_HOME>/wlp/usr/servers/<server_name>Server<#/>/resources/security/key.p12`

Procedure

1. Get the certificates from your CA and copy them to the OpenPages with Watson application server.
2. Log on to the OpenPages with Watson application server.
3. Import the certificate to OpenPages by running the following command:

```
keytool -importcert -v -alias <CERTIFICATE_ALIAS> -trustcacerts -file <CERTIFICATE_NAME>  
-keystore <STORE_PATH> -storetype PKCS12 -storepass <STORE_PASSWORD>
```

Where:

- `<CERTIFICATE_ALIAS>` type an alias for the certificate.
- `<CERTIFICATE_NAME>` is the file name of the certificate.
- `<STORE_PATH>` is the full path and file name of the Liberty keystore on the application server. For example: `<OP_HOME>/wlp/usr/servers/<server_name>Server<#/>/resources/security/key.p12`
- `<STORE_PASSWORD>` is the password of the Liberty keystore on the application server.

For more information, see [Adding trusted certificates in Liberty in the WebSphere Liberty documentation](#).

4. Restart the OpenPages with Watson services.

What to do next

After you import the CA certificates, configure the application properties files to use the TLS protocol. Do the following tasks:

- [“Updating properties files so web browsers use the HTTPS protocol and TLS ports” on page 653](#)
- [“Configuring Cognos to connect to OpenPages by using TLS” on page 665](#)

After you install new server certificates, you might need to install the CA root and intermediate certificates into several additional locations, if the certificates are not from a trusted third party. For example, if the certificate authority is an internal authority for your enterprise, or you are using self-signed certificates, you need to do additional steps. Do the following tasks:

- [“Importing the CA certificate for the Java Runtime Environment of IBM Cognos Analytics” on page 652](#)
- [“Installing CA certificates for all client browsers” on page 652](#)

Importing the CA certificate for the Java Runtime Environment of IBM Cognos Analytics

Use the Keytool command to import the Certificate Authority (CA) certificate that issued the certificates for IBM OpenPages with Watson into the Java JRE environment on each reporting server.

Before you begin

On each reporting server, \$JAVA_HOME/bin must be set in the PATH system environment variable. To verify that Java is in the PATH variable, run the following command:

```
java -version
```

If you get the following error, Java is not in the PATH variable: Command not found.

Tip: To check what certificates are in the keystore, you can use the following command:

```
keytool -list -v -keystore <JAVA_HOME>/lib/security/cacerts
```

Procedure

1. Log on to each IBM Cognos Analytics server as a user with administrative privileges.
2. Open a shell or command prompt. If you are using Windows, open the command prompt as an administrator.
3. Back up the <JAVA_HOME>/lib/security/cacerts file, where <JAVA_HOME> is the location of the JRE, for example /opt/ibm/java-x86_64-80/jre.
4. Go to the <JAVA_HOME>/bin directory
5. Type the following Keytool command to import the OpenPages root certificate into the cacerts keystore.

```
keytool -importcert -alias <certificate_name> -trustcacerts  
-file <file_name> -keystore <JAVA_HOME>/lib/security/<keystore_name>
```

For example, the following Keytool command imports the rootca certificate from the trustedcafename.cer file into the cacerts keystore file:

```
keytool -importcert -alias rootca -trustcacerts  
-file trustedcafename.cer -keystore /opt/ibm/java-x86_64-80/jre/lib/security/cacerts
```

6. Enter the password for the keystore.

The default password is changeit.

7. Enter Yes to trust the certificate.

What to do next

If you are using self-signed certificates for OpenPages that are not issued by a known CA, you must import the self-signed root certificate from any OpenPages server connected to the current Cognos server. Use the following Java keytool command to import the certificates into the keystore.

```
keytool -importcert -alias <certificate_name> -trustcacerts -file <file_name>  
-keystore <keystore_name>
```

Installing CA certificates for all client browsers

If your organization uses its own certificate authority (CA), most browsers will not trust the certificates. After you configure the web server for TLS, browsers might display a certificate exception. Users must accept the exception to access OpenPages.

Updating properties files so web browsers use the HTTPS protocol and TLS ports

After you configure the web server for TLS, edit the properties files to ensure that browsers use the HTTPS protocol and TLS ports. Do this task on the admin application server and all non-admin application servers.

About this task

In a load balanced environment, the values are the fully qualified domain name of the load balancer and its port number.

Procedure

1. Log on to each IBM OpenPages with Watson application server as a user with administrative privileges.
2. On Windows computers, start a Command Prompt window with the **Run as administrator** option. On Linux computers, open a shell.
3. Go to the <OP_HOME>/aurora/conf directory.
4. Open the aurora.properties file in a text editor.
 - a) Edit the following line. Change http to https and change <port> to the TLS port number.

```
application.url.path=http\://<server_name>\:<port>/openpages
```

Note: In a load balanced environment, the application.url.path value is the fully qualified domain name of the load balancer and its port number.

- b) Save and close the file.
5. Open each Server<#>-sosa.properties file in a text editor.
 - a) Edit the following line. Change http to https and change <port> to the TLS port number.

```
application.url.path=http\://<server>\:<port>/openpages
```

Note: In a load balanced environment, the application.url.path value is the fully qualified domain name of the load balancer and its port number.

- b) Save and close the file.
6. Open each Server<#>-server.properties in a text editor.
 - a) Edit the following lines. Change the http to https and change <port> to the TLS port number.

```
webclient.http.server.protocol=https  
webclient.http.server.port=<port>
```

- b) Save and close the file.
7. Restart all OpenPages application servers.
For more information, see [Chapter 25, “Starting and stopping servers,” on page 709](#).
8. Log in to OpenPages as an administrator.
9. Click  > **System Configuration** > **Settings**.
10. Update the following settings. For each setting, change http to https and change <port> to the TLS port number.
 - **Platform > Reporting > Cognos Dispatcher Service URL**
 - **Platform > Reporting > Cognos Logout URL**

Enabling secure session cookies on WebSphere Liberty

Enable or disable the cookieSecure setting on all application servers in your environment.

A secure session cookie informs the browser to send the session cookie back only over an HTTPS (encrypted HTTP) connection. This ensures that the cookie identifier is secure and is used only with IBM OpenPages with Watson when using HTTPS connections. When this feature is enabled, session cookies over an HTTP connection no longer work.

Procedure

1. Log on to the application server.

2. Edit the following file:

```
<OP_HOME>/wlps/usr/servers/<server_name>Server</>/configDropins/overrides/op-apps.xml
```

3. Locate the httpSession element. If it does not exist, create it.

4. Add the cookieSecure attribute to the httpSession element.

For example:

```
<httpSession cookieSecure="true" />
```

5. Locate the webAppSecurity element. If it does not exist, create it.

6. Add the ssoRequiresSSL attribute to the webAppSecurity element.

For example:

```
<webAppSecurity ssoRequiresSSL="true"/>
```

7. Restart the application server.

8. Repeat these steps on each application server.

TLS configuration for Microsoft Internet Information Services

In most environments, traffic to and from IBM Cognos Analytics passes through a web server. You can configure the Microsoft Internet Information Services web server for TLS. Microsoft Internet Information Services requires a certificates snap-in.

Procedure

1. Log on to each IBM Cognos Analytics server as a user with administrative privileges.

2. Start the Microsoft Management Console.

In the search box on the taskbar, type mmc, and press **Enter**.

3. In the **MMC** dialog box, click **File > Add/Remove Snap-Ins**.

4. In the **Available snap-ins** list, double-click **Certificates**.

5. In the **Certificates Snap-ins** dialog box, select **Computer account**, and then click **Next**.

6. In the **Select Computer** dialog box, select **Local Computer**, and then click **Finish**.

7. Click **OK** to close the dialog box.

Generating a key pair and request using Microsoft Internet Information Services

Use the reporting server to generate the key pair and specify the keystore in Microsoft Internet Information Services

Procedure

1. Log on to the primary reporting server as a user with administrative privileges.

2. In the Microsoft Management Console dialog box on the reporting server, expand the **Certificates** and select **Personal**.
3. In the **Actions** panel, right-click the **Certificates** icon and select **All Tasks > Advanced Options > Create Custom Request**.
4. In the **Certificate Enrollment** dialog box, click **Next**.
5. On the **Select Certificate Enrollment Policy** pane, select **Proceed without enrollment policy**, and click **Next**.
6. On the **Custom request** pane, accept the default values of **CNG key** and **PKCS#10**, and click **Next**.
7. In the **Certificate Information** pane, click the **Details** icon, and click **Properties**.
8. In the **Certificate Properties** dialog box, click the **Subject** tab to supply details for the certificate's Distinguished Name.
9. To specify a common name and organization value.
 - a) In the **Type** list, select **Common Name**, and enter a value for the certificate common name, and click **Add**.
 - b) Select **Organization** in the **Type** list and enter a value for the certificate common name, and click **Add**.
10. Click the **Private Key** tab and then:
 - a) Click the arrow next to **Key Options**, and select **Make private key exportable**.
 - b) Click the arrow next to **Select Hash Algorithm**, select **sha1** from the **Hash Algorithm** list, and click **OK**.
11. In the **Certificate Information** pane, click **Next**.
12. In the **Certificate Enrollment** pane:
 - a) Click **Browse** and in the **Save as** dialog box, enter a name for the certificate request file in the **File name** field. Use a .csr extension.
 - b) From the **Save as type** list, select **All Files**, and then click **Save**.
13. Click **Finish**.
14. Close the Microsoft Management Console.

Submitting a Certificate Signing Request for your web server

Submit the Certificate Signing Request to a Certificate Authority for approval.

Procedure

1. Download the approved root and server certificates to a local directory, such as the OpenPagesDomain directory.
2. Check that the certificates are named to distinguish the root from the server certificate.
3. Follow the instructions provided by the Certificate Authority.

Importing the root certificate into Microsoft Internet Information Services

You must import the root certificate into Microsoft Internet Information Services on the primary Cognos system and all secondary Cognos systems.

Procedure

1. Log on to each Cognos server as a user with administrative privileges.
2. Start the Microsoft Management Console (MMC).
 - a) Click the Windows **Start** menu.
 - b) Type mmc in the search box and press **Enter**.
3. In the **MMC** dialog box, click **File > Add/Remove Snap-Ins**.

4. In the **Available snap-ins** list, double-click **Certificates**.
5. In the **Certificates Snap-ins** dialog box, select **Computer account**, and click **Next**.
6. In the **Select Computer** dialog box, select **Local Computer**, and click **Finish**.
7. In the **MMC** dialog box, expand **Certificates** and select **Trusted Root Certification Authorities**.
8. In the **Actions** panel, right-click the **Certificates** icon and select **All Tasks > Import**.
9. In the Certificate Import wizard, click **Next**.
10. On the **File to Import** pane, click **Browse** to locate the CA certificate, and then click **Next**.
11. On the **Certificate Store** pane, select **Place all certificates in the following store > Trusted Root Certification Authorities**, and click **Next**.
12. On the **Completing the Certificate Import** wizard screen, click **Finish**.
13. Repeat these steps to import any intermediate certificates required by your Certificate Authority.

What to do next

If you are using self-signed certificates for OpenPages with Watson and Cognos, that are not issued by a known Certificate Authority, you must import the OpenPages signed root certificate from any OpenPages server connected to the current Cognos server. Use the following Java keytool command to import the certificates into the keystore.

```
keytool -importcert -alias certificate_name -trustcacerts -file file_name
-keystore keystore_name
```

Adding the TLS binding for Microsoft Internet Information Services

To bind the root certificate to the web server use Cognos on the primary Cognos system and all secondary Cognos systems.

Procedure

1. On the Cognos server, open the Windows Internet Information Services Manager.
Click **Start > Windows Administrative Tools > Internet Information Services (IIS) Manager**.
2. Expand the folder structure for the server that you want to configure, and then select **Sites**.
3. In the **Sites** pane, select the website to configure.
4. In the **Action** panel, select **Bindings**.
5. In the **Site Bindings** dialog box, select **HTTPS** and click **Edit**.

TLS configuration for Apache Web Server

To use TLS between IBM OpenPages with Watson applications and Apache Web Server, some configuration is required. For example, you must generate a keystore and a keypair, generate a certificate signing request, and establish the root of trust.

Generating a key pair and request using Cognos

Use Cognos to generate the key pair and specify the keystore for Apache Web Server on the primary Cognos system.

Procedure

1. Log on to the reporting server as a user with administrative privileges.
Note: For Linux systems, log in as a non-root user, such as the `opuser` user that you created for the IBM OpenPages with Watson installation.
2. Open a Linux shell, or Windows command prompt.
3. Go to the `bin` directory in the web server home directory.

4. Enter the following commands to generate a certificate request:

Windows:

```
openssl req -new -sha1 -newkey rsa:1024 -config %APACHE_HOME%\conf\  
openssl.cnf -nodes -keyout server_pkey.key  
-out certreq.csr
```

Linux:

```
openssl req -new -sha1 -newkey rsa:1024 -config $APACHE_HOME/conf/  
openssl.cnf -nodes -keyout server_pkey.key  
-out certreq.csr
```

5. Open the httpd.conf file using a text editor.

- a) Uncomment the following line.

```
LoadModule ssl_module modules/mod_ssl.so  
Secure (SSL/TLS) connections  
Include conf/extra/httpd-ssl.conf
```

6. Save and close the file.

Submitting a Certificate Signing Request for your web server

Submit the Certificate Signing Request to a Certificate Authority for approval.

Procedure

1. Download the approved root and server certificates to a local directory, such as the OpenPagesDomain directory.
2. Check that the certificates are named to distinguish the root from the server certificate.
3. Follow the instructions provided by the Certificate Authority.

Importing the root certificate into Apache web server

You must import the root certificate into Apache web server on the primary Cognos system and all secondary Cognos systems.

Procedure

1. Log on to the reporting server as a user with administrative privileges.
Note: Log on as a non-root user, such as the opuser user you created for the IBM OpenPages with Watson installation.
2. Go to the <Apache_Home>/conf/extra directory.
3. Open the httpd-ssl.conf file in a text editor.
4. Under **Server Certificate**, uncomment the **SSLCertificateFile** parameter, and enter the path to the PEM encoded certificate.
5. Under **Server Private Key**, uncomment the **SSLCertificateKeyFile** parameter, and enter the path to the keyfile on this server.
6. Under **Certificate Authority (CA)**, uncomment the **SSLCACertificateFile** parameter, and enter the path to the root certificate.
7. Save and close the file.

What to do next

If you are using self-signed certificates for OpenPages and Cognos that are not issued by a known Certificate Authority, you must import the OpenPages self-signed root certificate from any OpenPages

server connected to the current Cognos server. Use the following Java **keytool** command to import the certificates into the keystore.

```
keytool -importcert -alias certificate_name -trustcacerts -file file_name  
-keystore keystore_name
```

Importing the server certificate into Apache web server

You must import the server certificate from the Certificate Authority into Apache web server on the primary Cognos system and all secondary Cognos systems.

Procedure

1. Log on to the reporting server as a user with administrative privileges.
Note: Log on as a non-root user, such as the opuser user you created for the IBM OpenPages with Watson installation.
2. Go to the <Apache_Home>/conf/extra directory.
3. Open the httpd-ssl.conf file in a text editor.
4. Under **Server Certificate**, uncomment the **SSLCertificateFile** parameter, and enter the path to the PEM encoded certificate.
5. Under **Server Private Key**, uncomment the **SSLCertificateKeyFile** parameter, and enter the path to the keyfile on this server.
6. Under **Certificate Authority (CA)**, uncomment the **SSLCACertificateFile** parameter, and enter the path to the root certificate.

TLS configuration on a Linux load balancer server

To use TLS on a Linux-based load-balancing server that is running IBM HTTP Server (IHS) in IBM OpenPages with Watson, some configuration is required. For example, you must generate a keystore and a keypair, and generate a certificate signing request, and establish the root of trust.

Generating a keystore and key pair using the iKeyman tool

If you are using IBM HTTP Server as your web server, generate a key pair using the iKeyman tool on the load balance server.

Procedure

1. Log on to the load balance server as a user with administrative privileges.
2. Start iKeyman by running the following command:

IHS_root/bin/ikeyman

Where *IHS_root* is the location of the IHS.

The default location is *IHS_root* is /usr/IBM/HTTPServer/.

3. Create the keystore file to store the key pair.
 - a) Select **Key Database File > New**.
 - b) In the dialog box that displays, select **CMS** from the **Key database type** list.
 - c) In the **File Name** field, enter a file name for the new key database file.
 - d) In the **Location** field, enter the location where you want to store the keystore file, and click **OK**
For example: *usr/IBM/HTTPServer/bin*.
 - e) In the **Password Prompt** dialog box that displays, enter a password for the keystore. Re-enter the password.

- f) In iKeyman, select **Stash password to file** to create a .sth file. This file encrypts and stores the keystore password which is assigned an expiration time. You must change the password periodically.
- g) Click **OK**.

Generating a certificate signing request file using the iKeyman tool

If you require an authorized certificate from a trusted third-party certificate authority, you can use the iKeyman tool to generate the required certificate signing request.

Procedure

1. Log on to the load balance server as a user with administrative privileges.
2. Start iKeyman by running the following command: *IHS_root/bin/ikeyman*
Where *IHS_root* is the location of the IBM HTTP Server installation. The default location is /usr/IBM/HTTPServer/.
3. In the iKeyman tool, open the keystore created in Step 2.
 - a) Select **Key Database File > Open**.
 - b) Specify the type of keystore. The default type is **CMS**.
 - c) In the **File Name** and **Location** fields, enter the name and path to the keystore. You can also click **Browse** to locate the keystore, and click **OK**.
 - d) In the **Password Prompt** dialog box, enter the password for the keystore, and click **OK**.
4. Generate the certificate request for the open keystore.
 - a) Select **Create > New Certificate Request**.
 - b) In the **Create New Key and Certificate Request** dialog box, in the **Key Label** field, provide an identifier for the certificate.
 - c) In the **Key Size** list, select a key length for the certificate. The key size determines the strength of the encryption.
 - d) From the **Signature Algorithm** list, select an algorithm to apply to the certificate.
 - e) Provide the **dname** information to identify the certificate. Enter the values as appropriate.
commonName
organization
organizationUnit
localityName
stateName
country
 - f) Click **OK** to generate the request. A certificate request in the .arm format is created and saved to the specified location.

Submitting a Certificate Signing Request to a Certificate Authority running IBM HTTP

To submit the Certificate Signing Request, follow the instructions that are provided by the Certificate Authority. Depending on the instructions, you need to either copy and paste the content of the CSR to the text area or attach the CSR file.

Importing the Root and Signed Server Certificates using the iKeyman tool

You must install a signed certificate from a third-party certificate authority or self-signed certificates in both the keystore created and the keystore used by IBM HTTP Server. You must install a server certificate into the keystore created.

Procedure

1. Log on to the load balance server as a user with administrative privileges.
2. Start iKeyman by running the following command: *IHS_root/bin/ikeyman*
Where *IHS_root* is the location of the IHS. The default location is /usr/IBM/HTTPServer/.
3. In the iKeyman tool, open the keystore you created in Step 2.
 - a) Select **Key Database File > Open**.
 - b) Specify the type of keystore, by default **CMS**.
 - c) In the **File Name** and **Location** fields, enter the name and path to the keystore.
 - d) In the **Password Prompt** dialog box, enter the password for the keystore.
4. Import the signed CA certificate.
 - a) In the **Key database content** list, select **Signer Certificates**, and click **Add**.
 - b) In the **Open** window, in the **File Name** and **Location** fields, enter the name and path to the keystore.
 - c) In the **Enter a Label** dialog box that displays, in the **Enter a label for the certificate** field, enter a name for the certificate.
5. Select **Key Database File > Close**.
6. In the iKeyman tool, open the plugin-key.kdb keystore.
 - a) Select **Key Database File > Open**.
 - b) Specify the type of keystore. The default type is CMS.
 - c) In the **File Name** and **Location** fields, enter the name and path to the keystore.
The default directory for the plugin-key.kdb keystore is <*IHS root*>/Plugins/config/*server_name*/plugin-key.kdb, and click **OK**.
 - d) In the **Password Prompt** dialog box, enter the password for the keystore. The default password is **WebAS**, and click **OK**.
7. Select **Signer Certificates** in the **Key database content** list, and click **Add**.
8. In the **Add CA's Certificate from a file** window, enter the following information.
9. In the **Data type** list, select Base64-encoded ASCII data.
10. In the **File Name** and **Location** fields, enter the name and path to the keystore.
11. In the **Enter a Label** dialog box and the **Enter a label for the certificate** field, enter a name for the certificate.

Editing the Apache configuration file on IBM HTTP server

You must edit the httpd.conf file on the load balancer server for the IBM HTTP server.

Procedure

1. On Windows computers, start a Command Prompt window with the **Run as administrator** option. On Linux computers, open a shell.
2. Go to the <*IHS root*>/conf directory.
3. Open the httpd.conf file in a text editor.
 - a) Uncomment the following in the file.

```
LoadModule was_app22_module modules/mod_was_ap22_http.so
LoadModule negotiation_module module8s/mod_negotiation.so
```

b) Uncomment the following lines in the file and add any missing lines.

```
Listen 443
<VirtualHost *:443>
ServerName <server_name>
SSLEnable
SSLProtocolDisable SSLv2
SSLClientAuth None
<Directory />
Options FollowSymLinks
AllowOverride None
Order allow,deny
Allow from all
</Directory>
</VirtualHost>
SSLDisable
KeyFile <IHS_root>/<keystore_name>.kdb
```

c) Add the following line to point to the WebSphere plug-in Configuration.

```
WebSpherePluginConfig
<IHS root>/Plugins/config/<server_name>/plugin-cfg.xml
```

d) Save and close the file.

4. To apply the changes, restart the IBM HTTP Server.

TLS configuration for CommandCenter for an Apache load balancer server (Windows)

There are four procedures for the web server on any reporting server that handles external IBM OpenPages with Watson CommandCenter requests.

Generating a key pair and request with an Apache load balancer server

If you are using Apache as your load balancer server, you must generate a key pair and specify the keystore.

Procedure

1. Log on to the load-balancing server as a non-root user with administrative privileges.
2. On Windows computers, start a Command Prompt window with the **Run as administrator** option. On Linux computers, open a shell.
3. Go to the /bin directory in the web server home directory to use as the keystore.
4. To generate a certificate request, enter the following command :

- For Windows operating systems:

```
openssl req -new -sha1 -newkey rsa:1024 -config %APACHE_HOME%\conf\openssl.cnf
-nodes -keyout server_pkey.key -out certreq.csr
```

- For Linux operating systems:

```
openssl req -new -sha1 -newkey rsa:1024 -config $APACHE_HOME\conf\openssl.cnf
-nodes -keyout server_pkey.key -out certreq.csr
```

5. Open the httpd.conf file in a text editor and uncomment following line:

```
LoadModule ssl_module modules/mod_ssl.so
Secure (SSL/TLS) connections
```

```
Include conf/extra/httpd-ssl.conf
```

Submitting a CSR to a Certificate Authority for an Apache load balancer server

Submit the Certificate Signing Request (CSR) file for an Apache load balancer server to an appropriate Certification Authority (CA) for approval.

Procedure

1. Download the approved root and server certificates to a local directory, such as the OpenPagesDomain directory.
2. Check that the certificates are named to distinguish the root from the server certificate.
3. Follow the instructions provided by the Certificate Authority.

Importing the root certificates for an Apache load balancer server

You must import the root certificates into an Apache load balancer server.

Procedure

1. Log on to the load-balancing server as a non-root user with administrative privileges.
2. On Windows computers, start a Command Prompt window with the **Run as administrator** option. On Linux computers, open a shell.
3. Go to the <Apache_Home>/conf/extra directory.
4. Open the httpd-ssl.conf file in a text editor.
5. Under **Server Certificate**, uncomment the **SSLCertificateFile** parameter, and enter the path to the PEM encoded certificate.
6. Under **Server Private Key**, uncomment the **SSLCertificateKeyFile** parameter, and enter the path to the key file on this server.
7. Under **Certificate Authority (CA)**, uncomment the **SSLCACertificateFile** parameter, and enter the path to the root certificate.
8. Save and close the file.

Editing the Apache configuration file on Apache load balancer server

To add TLS parameters for the Apache load balancer server, you must edit the httpd.conf file.

Procedure

1. Log on to load-balancing web server as a user with administrative privileges.
2. Stop the Apache web server.
3. Start a Command Prompt window by using the **Run as administrator** option.
4. Copy the <WLP_HOME>\server\plugin\win\32\mod_wl_22.so file to the <Apache_Home>\modules directory.
Copy C:\Oracle\Middleware\wlserver_10.3\server\plugin\win\32\mod_wl_22.so to C:\Program Files\Apache Software Foundation\Apache2.2\conf
5. Go to the <Apache_Home>\conf\ directory.
6. Open the httpd.conf file and locate the parameters added to the end of the file for SSL. See the following example of these parameters.
 - a) Before the first **<Location />** parameter, add the following parameter.

```
<IfModule ssl_module>
SSLRandomSeed startup builtin
SSLRandomSeed connect builtin
```

```
</IfModule>
```

- b) In the **<Location />** parameter, add the location of the trusted CA certificate file.

TLS configuration for Cognos for IBM HTTP Server

If you use IBM HTTP Server (IHS) as a web server for Cognos, some configuration is required. For example, you must generate a keystore and key pair, and generate a certificate signing request, and submit a Certificate Signing Request (CSR).

Generating a keystore and key pair using the iKeyman tool

If you are using IBM HTTP Server as your web server, generate a key pair using the iKeyman tool on the reporting server.

Procedure

1. Log on to the reporting server as a user with administrative privileges.
2. Start iKeyman by running the following command:

IHS_root/bin/ikeyman

Where *IHS_root* is the location of the IHS.

The default location is *IHS_root* is */usr/IBM/HTTPServer/*.

3. Create the keystore file to store the key pair.
 - a) Select **Key Database File > New**.
 - b) In the dialog box that displays, select **CMS** from the **Key database type** list.
 - c) In the **File Name** field, enter a file name for the new key database file.
 - d) In the **Location** field, enter the location where you want to store the keystore file, and click **OK**
For example: *usr/IBM/HTTPServer/bin*.
 - e) In the **Password Prompt** dialog box that displays, enter a password for the keystore. Re-enter the password.
 - f) In iKeyman, select **Stash password to file** to create a *.sth* file. This file encrypts and stores the keystore password which is assigned an expiration time. You must change the password periodically.
 - g) Click **OK**.

Generating a certificate signing request file using the iKeyman tool

If you require an authorized certificate from a trusted third-party certificate authority, you can use the iKeyman tool to generate the required Certificate Signing Request.

Procedure

1. Log on to the reporting server as a user with administrative privileges.
2. Start iKeyman by running the following command: *IHS_root/bin/ikeyman*

Where *IHS_root* is the location of the IBM HTTP Server installation. The default location is */usr/IBM/HTTPServer/*.

3. In the iKeyman tool, open the keystore created in Step 2.
 - a) Select **Key Database File > Open**.
 - b) Specify the type of keystore. The default type is **CMS**.
 - c) In the **File Name** and **Location** fields, enter the name and path to the keystore. You can also click **Browse** to locate the keystore, and click **OK**.
 - d) In the **Password Prompt** dialog box, enter the password for the keystore, and click **OK**.

4. Generate the certificate request for the open keystore.
 - a) Select **Create > New Certificate Request**.
 - b) In the **Create New Key and Certificate Request** dialog box, in the **Key Label** field, provide an identifier for the certificate.
 - c) In the **Key Size** list, select a key length for the certificate. The key size determines the strength of the encryption.
 - d) From the **Signature Algorithm** list, select an algorithm to apply to the certificate.
 - e) Provide the **dname** information to identify the certificate. Enter the values as appropriate.
 - commonName
 - organization
 - organizationUnit
 - localityName
 - stateName
 - country
 - f) Click **OK** to generate the request. A certificate request in the .arm format is created and saved to the specified location.

Submitting a CSR to a Certificate Authority

To submit the Certificate Signing Request, follow the instructions that are provided by the Certificate Authority. Depending on the instructions, you need to either copy and paste the content of the CSR to the text area or attach the CSR file.

Downloading and importing the root and signed server certificates using the iKeyman tool

You must install a signed certificate from a third-party Certificate Authority or self-signed certificates in both the keystore created and the keystore used by IBM HTTP Server. You must install a server certificate into the keystore created.

Procedure

1. Follow the instructions provided by the Certificate Authority to download the root and signed server certificates.
2. Download the approved root and Certificate Authority certificates to a local directory.
3. Check that the certificates are named to distinguish the root from the Certificate Authority certificate.
4. Log on to the reporting server as a user with administrative privileges.
5. Start iKeyman by running the following command: <*IHS_root*>/bin/ikeyman
Where <*IHS_root*> is the location of the IHS. The default location is /usr/IBM/HTTPServer/.
6. In the iKeyman tool, open the keystore you created for Cognos.
 - a) Select **Key Database File > Open**.
 - b) Specify the type of keystore, by default **CMS**.
 - c) In the **File Name** and **Location** fields, enter the name and path to the keystore.
 - d) In the **Password Prompt** dialog box, enter the password for the keystore.
7. Import the root certificate.
 - a) In the **Key database content** list, select **Signer Certificates**, and click **Add**.
 - b) In the **Open** window, in the **File Name** and **Location** fields, enter the name and path to the root certificate file.
 - c) In the **Enter a Label** dialog box that displays, in the **Enter a label for the certificate** field, enter a name for the root certificate.
8. Import CA signed certificate.

- a) In the **Key database content** list, select **Personal Certificates**, and click **Receive**.
- b) In the **Open** window, in the **File Name** and **Location** fields, enter the name and path to the CA signed certificate file.
When the import is complete, a status message is displayed.
- c) Click **OK**.

Updating the Apache configuration file on IBM HTTP server

You must update the httpd.conf file and restart the server.

Procedure

1. On Windows computers, start a Command Prompt window with the **Run as administrator** option. On Linux computers, open a shell.
2. Go to the <IHS_root>/conf directory.
3. Open the httpd.conf file using a text editor.

- a) Uncomment the following in the file.

```
LoadModule ibm_ssl_module modules/mod_ibm_ssl.so
Listen 443
<VirtualHost *:443>
SSLEnable
</VirtualHost>
KeyFile /home/opuser/IBM/HTTPServer/<yourkeystore.kdb>
SSLDisable
```

- b) Save and close the file.

Note: You must also replace <yourkeystore.kdb> with your keystore file and replace port 443 with your TLS/SSL port for IBM HTTP Server.

4. To apply the changes, restart the IBM HTTP Server.

Configuring Cognos to connect to OpenPages by using TLS

If IBM OpenPages with Watson is configured for TLS, you must configure the properties file to use the OpenPages HTTPS address and TLS port. Modify the OpenPages properties file to use HTTPS and the TLS port on the primary Cognos server and on each secondary Cognos server.

Before you begin

Set up IBM HTTP Server (IHS) as a web server for Cognos. For more information, see “[TLS configuration for Cognos for IBM HTTP Server](#)” on page 663.

Procedure

1. Log on to the Cognos server as a user with administrative privileges.
- Note:** For Linux, log on as a non-root user, such as the opuser user that you created for the OpenPages with Watson installation.
2. On Windows computers, start a Command Prompt window with the **Run as administrator** option. On Linux computers, open a shell.
 3. Go to the following directory: <Cognos_Home>/configuration
 4. Open the OpenPagesSecurityProvider_OpenPagesSecurityRealm.properties file in a text editor.
 5. Edit the following lines to change the http to https and update the port number.

```
openpages.application.url=http\://<server>:<port>/openpages
```

6. Restart all Cognos servers.

For more information, see [Chapter 25, “Starting and stopping servers,” on page 709](#).

TLS configuration for Db2

You can configure a secure connection between IBM Db2 and IBM OpenPages with Watson.

You can configure a Transport Layer Security (TLS) connection between the database server and the application servers, and between the database server and the reporting servers.

You can also configure a secure connection between the database server and the search server. For more information, see [“Enabling a secure connection between the search server and the database server” on page 676](#).

Setting up SSL on the database server (Db2)

You can configure a secure connection between the OpenPages database on IBM Db2 and the OpenPages application servers. You can also set up a secure connection between the OpenPages database and Cognos. First, you need to set up SSL on Db2.

Note: If you already have a keystore for SSL, skip this task. Go to [“Configuring application and reporting servers to use a secure connection to the database \(Db2\)” on page 667](#).

Procedure

1. Stop all application servers and all reporting servers.

2. Stop the OpenPages database.

a) Log on to the database server as the OpenPages database instance owner (by default db2inst1 on Linux or db2admin on Windows).

b) Run the following commands:

```
db2 deactivate db <op_database_name>
db2stop
```

Replace *<op_database_name>* with the name of the OpenPages database, for example opx.

3. Enable SSL (TLS) on the database server.

Do these steps as the OpenPages database instance owner.

a) Create or choose a keystore directory to store the database key.

For example: /home/db2inst1/sqllib/security/keystore/

b) Go to the Db2 gskit/bin directory. This is the directory where the gsk8capicmd_64 utility is stored.

For example: /opt/ibm/db2/V11.5/gskit/bin/ or /home/db2inst1/sqllib/gskit/bin/.

Tip: The PATH environment variable might already include the gskit/bin directory.

c) Run the following command:

```
gsk8capicmd_64 -keydb -create -db <keystore_directory>/<db_key_name>.p12 -pw
"<db_key_password>" -type pkcs12 -stash
```

- Replace *<keystore_directory>* with the directory in step [“3.a” on page 666](#).
- Replace *<db_key_name>* with the name of the keystore file (.p12).
- Replace *<db_key_password>* with the password of the keystore.

On Linux for example:

```
./gsk8capicmd_64 -keydb -create -db /home/db2inst1/sqllib/security/keystore/opx_db.p12
-pw "mypassword" -type pkcs12 -stash
```

d) Run the following command:

```
gsk8capicmd_64 -cert -create -db "<keystore_directory>/<db_key_name>.p12" -pw "<db_key_password>" -stashed -label "<certificate_name>" -dn "CN=<host_name>, O=<company>, L=<city>, ST=<state>, C=<country>" -size 2048 -sigalg SHA256withRSA
```

On Linux for example:

```
./gsk8capicmd_64 -cert -create -db "/home/db2inst1/sqllib/security/keystore/opx_db.p12" -pw "mypassword" -stashed -label "opx_selfsigned_cert" -dn "CN=mydbserver, O=IBM Corp, L=Boston, ST=MA, C=US" -size 2048 -sigalg SHA256withRSA
```

You now have a self-signed certificate for the OpenPages database.

4. Update Db2 configuration parameters.

- Run the following commands in the following sequence. Wait for each command to complete before you run the next command:

```
db2 update dbm cfg using SSL_SVR_KEYDB <keystore_directory>/<db_key_name>.p12  
db2 update dbm cfg using SSL_SVR_STASH <keystore_directory>/<db_key_name>.sth  
db2 update dbm cfg using SSL_SVR_LABEL <certificate_name>  
db2 update dbm cfg using SSL_SVCENAME <db2_ssl_port>  
db2set -i <db_user_name> DB2COMM=SSL,TCPIP
```

For example:

```
db2 update dbm cfg using SSL_SVR_KEYDB /home/db2inst1/sqllib/security/keystore/opx_db.p12  
db2 update dbm cfg using SSL_SVR_STASH /home/db2inst1/sqllib/security/keystore/opx_db.sth  
db2 update dbm cfg using SSL_SVR_LABEL opx_selfsigned_cert  
db2 update dbm cfg using SSL_SVCENAME 50051  
db2set -i db2inst1 DB2COMM=SSL,TCPIP
```

- If you have another database server, repeat these steps on the other database server.

5. Start the OpenPages database.

- Log on to the database server as the OpenPages database instance owner (by default db2inst1 on Linux or db2admin on Windows).
- Run the following commands:

```
db2start  
db2 activate db <op_database_name>
```

6. Configure your firewall to allow connections to the SSL port for Db2.

What to do next

Configure WebSphere Liberty to connect to Db2 by using the secure connection. For more information, see [“Configuring application and reporting servers to use a secure connection to the database \(Db2\)” on page 667](#).

Configuring application and reporting servers to use a secure connection to the database (Db2)

After you set up SSL on IBM Db2, configure WebSphere Liberty and Cognos to use the secure connection.

Before you begin

Ensure that you completed all steps in [“Setting up SSL on the database server \(Db2\)” on page 666](#).

Ensure that you know the SSL port number for Db2.

Procedure

- Log on to the admin application server as the OpenPages installation user (opuser).
- If you do not have the SSL certificate for Db2, run the following command:

```
openssl s_client -servername <db_server_url> -connect <db_server_url>:<db_server_ssl_port>
```

```
</dev/null 2>/dev/null | \
sed -ne '/-BEGIN CERTIFICATE-/,/-END CERTIFICATE-/p' > <directory>/db2.cert;
```

- Replace *<db_server_url>* with the fully qualified domain name (FQDN) of the database server.
- Replace *<db_server_ssl_port>* with the SSL port for Db2.
- Replace *<directory>* with the full path to a directory on the application server. This directory is where the certificate is saved.

3. Import the Db2 certificate to the Java keystore on the application server.

For example:

```
/opt/ibm/java-x86_64-80/jre/bin/keytool -import \
    -alias db2_ssl \
    -trustcacerts \
    -file /home/opuser/db2.cert \
    -keystore /opt/ibm/java-x86_64-80/jre/lib/security/cacerts \
    -storepass <Java_password>
```

4. Import the Db2 certificate to the Liberty keystore on the application server.

If you are using vertical application servers, do this step on each of them.

For example:

```
/opt/ibm/java-x86_64-80/jre/bin/keytool -import \
    -alias db2_ssl \
    -trustcacerts \
    -file /home/opuser/db2.cert \
    -keystore /home/opuser/IBM/OpenPages/wlp/usr/servers/OpenPagesNodeServer1Server1/
resources/security/key.p12 \
    -storetype PKCS12 \
    -storepass <password>
```

5. Modify the bootstrap.properties file.

- Open the following file in a text editor: *<OP_HOME>/wlp/usr/servers/<server_name>Server<#/>bootstrap.properties*
- Set the op.db2.ssl property to true.
- Update the op.db2.portNumber property with the SSL port number for Db2.

6. Modify the aurora.properties file.

- Open the following file in a text editor: *<OP_HOME>/aurora/conf/aurora.properties*
- Update the database.PORT property with the SSL port number for Db2.
- Update the database.URL property with the SSL port number for Db2.
Append :sslConnection=true; to the URL.

For example:

```
database.URL=jdbc\:db2\://op-appserver.ibm.com\:50001/OPX:sslConnection=true;
```

7. Import the Db2 certificate to the Java keystore on each reporting server.

For example, if you're using the Java that is provided with Cognos:

```
/usr/IBM/cognos/analytics(ibm-jre)/jre/bin/keytool -import \
    -alias db2_ssl \
    -trustcacerts \
    -file /home/opuser/db2.cert \
    -keystore <COGNOS_HOME>/ibm-jre/jre/lib/security/cacerts \
    -storepass <Java_password>
```

Or if you're using the Java that is provided with OpenPages:

```
/opt/ibm/java-x86_64-80/jre/bin/keytool -import \
    -alias db2_ssl \
    -trustcacerts \
    -file /home/opuser/db2.cert \
    -keystore /opt/ibm/java-x86_64-80/jre/lib/security/cacerts \
    -storepass <Java_password>
```

8. Configure the IBM Db2 database client to use the secure connection. Do this step on each application server and reporting server.

a) Import the Db2 certificate to the Java keystore that is bundled with the Db2 client software.

For example:

```
/home/opuser/sqllib/java/jdk64/jre/bin/keytool -import \
    -alias db2_ssl \
    -trustcacerts \
    -file /home/opuser/db2.cert \
    -keystore /home/opuser/sqllib/java/jdk64/jre/lib/security/cacerts \
    -storepass <password>
```

b) Create a keystore for the Db2 client.

For example:

```
gsk8capicmd -keydb -create -db /home/opuser/sqllib/security/keystore/ox_db.p12 -pw
"OpenPages1" -type pkcs12 -stash
db2 update dbm cfg using SSL_CLNT_KEYDB /home/opuser/sqllib/security/keystore/ox_db.p12
db2 update dbm cfg using SSL_CLNT_STASH /home/opuser/sqllib/security/keystore/ox_db.sth
```

c) Import the Db2 certificate.

For example:

```
gsk8capicmd -cert \
    -add \
    -db /home/opuser/sqllib/security/keystore/ox_db.p12 \
    -stashed \
    -label db2_ssl \
    -file /home/opuser/db2.cert \
    -format ascii \
    -fips
```

9. Recatalog the OpenPages node.

For example:

```
db2 uncatalog node openpage
db2 catalog TCPIP NODE openpage REMOTE op-dbserver.com server 50001 SECURITY SSL
db2cli writecfg add -dsn OPXSSL -database OPX -host op-dbserver.com -port 50001 -parameter
'SecurityTransportMode=SSL'
```

10. Restart the OpenPages application services.

11. Repeat steps “1” on page 667 to “10” on page 669 on each application server.

12. Update the database connection information in Cognos so that the reporting servers use SSL to connect to the OpenPages database.

a) Open **IBM Cognos Administration**. Select the **OpenPages data source** and edit the connection string.

For more information, see “[Update Db2 database connection references for Cognos](#)” on page 565.

b) Click the **JDBC** tab.

c) Change **Port number** to the SSL port number for Db2.

d) In the **JDBC Connection Parameter field**, type `sslConnection="true";`.

e) Save your changes and exit **IBM Cognos Administration**.

f) Restart the reporting servers.

Modifying the LDAP configuration file for LDAP over TLS

You must modify the authentication configuration file to enable the LDAP directory server that you are using.

The `aurora_auth.config` file contains three authentication modules:

- Openpages - the default internal user directory
- OpenpagesIP - a sample LDAP configuration for the Sun One Directory Server

- OpenpagesAD - a sample LDAP configuration for the Microsoft Active Directory Server

The only module that the IBM OpenPages with Watson system pays attention to is the module that is named Openpages. Therefore, you need to make a backup of the Openpages module, rename the OpenpagesIP or OpenpagesAD to Openpages, and then change the settings to reflect the settings of your LDAP server.

Procedure

1. Stop all OpenPages with Watson services.
2. Open and edit the `<OP_HOME>/aurora/conf/aurora_auth.config` file in a text editor.

Where:

`<OP_HOME>` is the installation location of the OpenPages with Watson application.

3. Find the Openpages module and change its name to OpenpagesDefault.
4. Modify either the OpenpagesIP or OpenpagesAD module name to Openpages.
 - If you are using a Microsoft Active Directory server, change the name of the OpenpagesAD module to Openpages.
 - If you are using a Sun One Directory Server, change the name of the OpenpagesIP module to Openpages.
 - If you are using a different LDAP server, you can use either of these modules. Choose a module to use as a template and change its name to Openpages.
5. Specify the correct values for the following properties in the module that you named Openpages:

provider.url

Change the value to the hostname and port number for the LDAP authentication server. For LDAP over TLS (LDAPS), the protocol is ldaps and the port is the LDAPS port number (by default, 636).

base_dn

The top level of the LDAP directory tree structure (Domain Name) on the LDAP server. If the users to be authenticated are located in multiple locations within your Active Directory structure, list all of the locations explicitly by using the distinguished names of the locations, each separated by a semi-colon.

For example:

```
base_dn="DC=LDAPTesting,DC=local;CN=Users,DC=LDAPTesting,DC=local;
OU=Auditors,OU=External Auditors,OU=Staff,DC=LDAPTesting,DC=local"
```

user.attr.id

The attribute name of the user identifier (for example, uid, cn, etc.).

Additional custom parameters

You can add additional custom parameters that are supported by the Java Naming and Directory Interface (JNDI). Precede a JNDI property with the `ctx.env.` prefix.

For example, if you want to use the JNDI property `com.sun.jndi.ldap.connect.timeout`, use `ctx.env.com.sun.jndi.ldap.connect.timeout=<value>` in the `aurora_auth.config` file.

For information about JNDI properties, see the [Java SE documentation](#).

For example:

```
Openpages
{
    com.openpages.aurora.service.security.namespace.LDAPLoginModule
        required debug=false
        provider.url="ldaps://myserver.company.com:636"
        security.authentication="simple"
        security.search.user.dn="cn=Directory Manager"
        security.search.user.credentials="openpages"
        base_dn="ou=people,o=IBM,c=US"
        user.attr.id="uid"
```

```
};
```

6. When you are finished editing the file, save your changes and exit.
7. Import the root certificate and any intermediate signer certificates for your LDAP server to the truststore on the OpenPages application servers.
For more information, see [“Importing signed CA certificates” on page 650](#).
8. Restart all services.

Results

You have configured the OpenPages with Watson system to use an external LDAP user authentication server over TLS.

Renewing TLS certificates for OpenPages with Watson

Periodically, TLS certificates need to be renewed and re-imported into your IBM OpenPages with Watson environment.

The process for renewing a certificate is similar to the process for installing new certificates. You create a new certificate request and import the signed certificate into the appropriate keystores. You do not need to repeat the steps for configuring TLS and changing property files for OpenPages with Watson, unless information contained in the certificate changes.

Certification Authorities provide instructions on how to submit renewal applications and import the signed certificates.

Renewing TLS certificates for Cognos environments on an IIS Web Server

Renew TLS certificates for Cognos environments for the web server on any reporting server that handles external Cognos traffic.

This information applies only to Windows environments.

Procedure

1. Generate a key pair and request.
 - a) Log on to the reporting server as a user with administrative privileges.
 - b) Launch the Internet Information Services Manager, by clicking **Start > Windows Administrative Tools > Internet Information Services (IIS) Manager**.
 - c) In the **Internet Information Services Manager**, select the application server you want to configure.
 - d) In the **Features** view, double-click **Server Certificates**.
 - e) In the **Actions** pane, click **Create Certificate Request** to launch the Request Certificate Wizard.
 - f) On the **Distinguished Name Properties** screen of the wizard:

Table 209. Distinguished Name Properties screen

In this text box	Do this
Common name	Type a name for the certificate.
Organization	Type the name of the organization in which the certificate will be used.
Organizational unit	Type the name of the organizational unit in the organization in which the certificate will be used.

Table 209. Distinguished Name Properties screen (continued)

In this text box	Do this
City/locality	Type the unabbreviated name of the city or locality where your organization or organizational unit is located.
State/province	Type the unabbreviated name of the state or province where your organization or organizational unit is located.
Country/region	Type the name of the country or region where your organization or organizational unit is located.

- g) Click **Next**.
 - h) On the **Cryptographic Service Provider Properties** screen, select a cryptographic service provider from the list:
 - Microsoft RSA SChannel Cryptographic Provider
 - Microsoft DH SChannel Cryptographic Provider
 - i) On the **Cryptographic Service Provider Properties** screen, select a bit length that can be used by the provider from the **Bit length** drop-down list.
By default, the RSA SChannel provider uses a bit length of 1024. The DH SChannel provider uses a bit length of 512. A longer bit length is more secure, but it can affect performance.
 - j) Click **Next**.
 - k) On the **File Name** page, in the **Specify a file name for the certificate** request field, use the **Browse** icon or type a name for the certificate file.
 - l) Click **Finish**.
2. Submit the Certificate Signing Request (CSR) to the Certification Authority (CA) for approval.
- a) Submit the CSR to your CA to renew the certificate. Follow the instructions provided by your CA on how to submit the CSR.
 - b) Download the approved root and CA certificates to a local directory. Make sure the certificates are named to distinguish the root from the CA certificate.
3. Install the signed certificate.
- Import the renewed server certificate into each reporting server by performing the following tasks:
- a) Log on to the reporting server as a user with administrative privileges.
 - b) Launch the Internet Information Services Manager, by clicking **Start > Windows Administrative Tools > Internet Information Services (IIS) Manager**.
 - c) In the **Internet Information Services Manager**, select the application server you want to configure.
 - d) In the **Features** view, double-click **Server Certificates**.
 - e) In the **Actions** pane, click **Complete Certificate Request**.
 - f) On the **Complete Certificate Request** screen:
 - In the **File name that contains the certification authority's** response field, use the **Browse** icon or type the path of the file that contains the signed certificate.
 - In the **Friendly name** field, type a recognizable name for the certificate.
 - Click **OK**.

Renewing TLS certificates for Cognos environments on an Apache Web Server

Perform these steps for the web server on any reporting server that handles external Cognos traffic.

Procedure

1. Log on to the reporting server as a user with administrative privileges.

Note: Log in as a non-root user, such as the user you created for the IBM OpenPages with Watson installation, for example: opuserx.

2. Perform the following tasks to renew your certificate(s):

- a) Generate a key pair and request.
- b) Submit the CSR to the CA for approval.
- c) Apache uses OpenSSL which requires the server keys and certificate locations be updated in `extras/httpd-ssl.conf`.

For more information, see [“TLS configuration for Apache Web Server” on page 656](#).

Renewing TLS certificates on application servers

To renew a TLS certificate for IBM OpenPages with Watson, create a new certificate signing request, submit it to a Certification Authority, and import the signed server certificate.

Procedure

1. Log on to cluster administrator server as a user with administrative privileges.

2. Create the certificate request.

For more information, see [“Generating a Certificate Signing Request file” on page 650](#).

3. Submit the request to the Certification Authority (CA).

- a) Submit the Certificate Signing Request (CSR) to your Certification Authority (CA) to renew the certificate. Follow the instructions provided by your CA on how to submit the CSR.
- b) Download the approved server and CA certificates. Make sure the certificates are named to distinguish the server from the CA certificate.

4. Import the certificate.

Import the renewed server certificate into each application server. For more information, see [“Importing signed CA certificates” on page 650](#).

Setting up a secure connection for the global search service

You can configure the IBM OpenPages with Watson global search service (Apache Solr) to use a secure connection with TLS. TLS ensures that all data that is passed between the application server and the Solr service remains private.

Before you begin

On the search server and application servers, `$JAVA_HOME/bin` must be set in the PATH system environment variable. To verify that Java is in the PATH variable, run the following command:

```
java -version
```

If you get the following error, Java is not in the PATH variable: Command not found.

About this task

If you are setting up the global search component in a test environment, do not enable TLS until you resolve all installation and configuration issues.

For more information about the commands that are used in this task, see the [Apache Solr documentation](#).

Important: IBM is not responsible for third-party content. At the time of publication, the information is correct.

Procedure

1. If the global search component is enabled, you must disable it.
 - a) Log on to OpenPages as a user with administrative privileges.
 - b) Click  > **System Configuration** > **Global Search** and click **Disable**.
2. Stop the global search services.
For more information, see “[Start or stop the global search services](#)” on page 712.
3. Create a certificate for the secure connection.
 - a) Go to the `<SEARCH_HOME>/solr/server/etc` folder and run the following command.

```
keytool -genkeypair -alias alias -keyalg key_algorithm  
-keysize keysize -keypass key_pass -storepass keystore_passwd  
-validity validity -keystore keystore.p12 -storetype PKCS12  
-ext ip_address -dname "CN=localhost, OU=Organizational Unit, O=Organization,  
L=Location, ST=State, C=Country"
```

In the following example, the command creates a self-signed certificate in a keystore that is named `solr-ssl.keystore.p12`. The keystore contains a key with an alias of `solr-ssl`, a keystore password of `secret`, a truststore password of `secret`. It specifies Subject Alternative Name (SAN) values of DNS:`host.company.com` and IP:`127.0.0.1,192.168.7.1` to include in the certificate. (SAN values are not mandatory, and might not be specified in your environment).

```
keytool -genkeypair -alias solr-ssl -keyalg RSA  
-keysize 2048 -keypass secret -storepass secret  
-validity 9999 -keystore solr-ssl.keystore.p12 -storetype PKCS12  
-ext SAN=DNS:host.company.com,IP:127.0.0.1,IP:192.168.7.1  
-dname "CN=localhost, OU=Organizational Unit, O=Organization, L=Location, ST=State,  
C=Country"
```

- b) Optional: If you need a PEM file, convert the PKCS12 format keystore, including the certificate and the key, into PEM format.

To run this command, `openssl` must be installed, and added to the PATH environment variable.

```
openssl pkcs12 -in <keystore.p12> -out <keystore.pem>
```

When you are prompted for the import password and PEM pass phrase, you can use the same password that you specified for the `<key_pass>` value in step 3a.

4. Export the certificate that you created in step 3.

```
keytool -exportcert -keystore <keystore> -alias <alias> -file <solr_certificate>
```

When you are prompted for the keystore password, type the password that you specified for the `<key_pass>` value in step 3a.

For example:

```
keytool -exportcert -keystore solr-ssl.keystore.p12 -alias solr-ssl -file solr_ssl.cert
```

5. Update the `solr.in` file.

- a) Edit the following file in a text editor:

Windows

```
<SEARCH_HOME>\solr\bin\solr.in.cmd
```

Linux

```
<SEARCH_HOME>/solr/bin/solr.in.sh
```

- b) Uncomment and set the following TLS properties.

```
SOLR_SSL_ENABLED=true  
SOLR_SSL_KEY_STORE=etc/keystore.p12  
SOLR_SSL_KEY_STORE_PASSWORD=keystore_passwd  
SOLR_SSL_TRUST_STORE=etc/keystore.p12  
SOLR_SSL_TRUST_STORE_PASSWORD=keystore_passwd  
SOLR_SSL_NEED_CLIENT_AUTH=false  
SOLR_SSL_WANT_CLIENT_AUTH=true  
SOLR_SSL_CHECK_PEER_NAME=true
```

On Windows, you might need to use `server/etc` as the path name for the `SOLR_SSL_KEY_STORE` and `SOLR_SSL_TRUST_STORE` properties.

6. Log in to the OpenPages application as a user with administrative privileges.

7. Click  > **System Configuration** > **Settings**.

8. Update the following settings to use `https` instead of `http`.

Platform > Search > Admin > Search Server Administration URL

Platform > Search > Index > Search Server URL

Platform > Search > Request > Search Server URL

9. Copy the certificate file that you exported in step 4 to the following directory on the application server.

`<JAVA_HOME>/lib/security`, where `<JAVA_HOME>` is the location of the JRE.

For example:

```
/opt/ibm/java-x86_64-80/jre/lib/security/solr_ssl.cert
```

10. Add the certificate to the IBM Java keystore on each application server.

a) On Windows computers, start a Command Prompt window with the **Run as administrator** option. On Linux computers, open a shell.

b) Back up the `<JAVA_HOME>/lib/security/cacerts` file, where `<JAVA_HOME>` is the location of the JRE, for example `/opt/ibm/java-x86_64-80/jre`.

c) Go to the `<JAVA_HOME>/bin` directory.

d) Update the `<JAVA_HOME>/lib/security/cacerts` file by running the following command.

```
keytool -importcert -alias <cert_alias> -keystore <JAVA_HOME>/lib/security/cacerts  
-file <solr_certificate>
```

When prompted, type the keystore password of the `cacerts` keystore. The default password is typically `changeit`.

For example:

```
keytool -importcert -alias solr-ssl -keystore /opt/ibm/java-x86_64-80/jre/lib/security/  
cacerts -file /opt/ibm/java-x86_64-80/jre/lib/security/solr_ssl.cert
```

e) Confirm that you want to trust the certificate.

11. Import the certificate to the IBM WebSphere truststore on each application server.

a) Log on to the OpenPages application server.

b) Run the following command:

```
keytool -importcert -v -alias <cert_alias> -file <solr_certificate>  
-keystore <keystore_path> -storetype PKCS12 -storepass <keystore_password>
```

For example:

```
keytool -importcert -v -alias solr-ssl  
-file /opt/ibm/java-x86_64-80/jre/lib/security/solr_ssl.cert  
-keystore /opt/IBM/OpenPages/wlp/usr/servers/app1Server1/resources/security/key.p12  
-storetype PKCS12 -storepass <STORE_PASSWORD>
```

For more information, see [Adding trusted certificates in Liberty in the WebSphere Liberty documentation](#).

- c) Restart all OpenPages services.
12. If the search server is installed on a different computer than the application server, add the certificate to the IBM Java keystore on the search server.
 - a) On Windows computers, start a Command Prompt window with the **Run as administrator** option.
On Linux computers, open a shell.
 - b) Go to the <JAVA_HOME>/bin directory and run the following command:

```
keytool -importcert -alias <alias> -keystore <JAVA_HOME>/lib/security/cacerts  
-file <SEARCH_HOME>/solr/server/etc/solr_certificate
```

For example:

```
keytool -importcert -alias solr-ssl -keystore /opt/ibm/java-x86_64-80/jre/lib/security/  
cacerts -file /opt/IBM/OpenPages/OPSearch/solr/server/etc/solr_ssl.cert
```

- c) When prompted, type the keystore password of the cacerts keystore. The default password is typically changeit.
13. Start the global search services.

For more information, see [“Start or stop the global search services” on page 712](#).

Enabling a secure connection between the search server and the database server

When you install the global search server, it uses a plain connection to communicate with the database server. If your organization requires that you use a TLS connection, you must complete these steps.

Procedure

1. Disable global search.
 - a) Log in to IBM OpenPages with Watson with administrative privileges.
 - b) Click  > **System Configuration** > **Global Search** and click **Disable**.
2. Configure TLS on the database server.
 - For configuring TLS on Db2, see [Configuring TLS client connections with Db2](#)
 - For configuring TLS on Oracle, see [21.8.1 Step 1: Configure Secure Sockets Layer on the Server](#)
3. On the search server, follow these steps to enable TLS:
 - a) If you are using Windows, open a command prompt with the **Run As administrator** option.
 - b) Go to the <SEARCH_HOME>/OPSearch/opsearchtools/ directory.
 - c) Enable TLS by running the following command.

```
opsearchtool.cmd|sh enableSSLDbConn -ssltruststorefile <path_to_client_keystore.jks>  
-ssltruststorepassword <your_JKS_password>
```

For example:

```
opsearchtool.cmd enableSSLDbConn -ssltruststorefile c:\keystore\client_keystore.jks  
-ssltruststorepassword JKSpassword
```
 - d) Edit the file <SEARCH_HOME>/OPSearch/opsearchtools/openpages_search.properties. Change the port number to the TLS port that your database server is using:
`OPSearchTool.DatabasePort = db_secure_port_number.`
4. Enable global search.
 - a) Log in to IBM OpenPages with Watson with administrative privileges.

- b) Click  > **System Configuration** > **Global Search** and click **Enable**.

Note: In some rare cases, you might need to pass additional parameters to the Java JRE. If this is the case, you can edit one of the following files to do so.

- For IBM Db2, edit <SEARCH_HOME>/OPSearch/opsearchtools/DatabasePropertyFile_DB2.properties
- For Oracle, edit <SEARCH_HOME>/OPSearch/opsearchtools/DatabasePropertyFile_Oracle.properties

Disabling the TLS database connection between the search server and the database server

If you need to disable the TLS connection between the search server and the database server, follow these steps.

Procedure

1. Disable global search.
 - a) Log in to IBM OpenPages with Watson with administrative privileges.
 - b) Click  > **System Configuration** > **Global Search** and click **Disable**.
2. Disable TLS on the database server.
3. Start global search.
 - a) Log in to IBM OpenPages with Watson with administrative privileges.
 - b) Click  > **System Configuration** > **Global Search** and click **Enable**.

Db2 native encryption

OpenPages with Watson supports Db2 native encryption.

This topic applies to Db2 on-premises.

You can set up Db2 native encryption after you install OpenPages.

For more information, see the [Db2 documentation](#)



Attention:

- Do not lose access to your main key (MK). If you lose access to the MK, you irrevocably lose access to the data in your encrypted database or database backup.
- The management of the encryption keys is entirely your organization's responsibility. The OpenPages application does not perform any actions that are related to the setup, control, rotation, backup, restore, or management of the encryption keys.

Oracle Transparent Data Encryption (TDE)

You can use Oracle Transparent Data Encryption (TDE) to encrypt the OpenPages and Cognos table spaces in the OpenPages database.

This task is optional.

Note: This task is for existing databases. You can also set up TDE when you do a fresh installation. For more information, see the *IBM OpenPages with Watson Installation and Deployment Guide*.

IBM OpenPages with Watson supports the ability to implement TDE, but TDE is an Oracle feature. You need to be familiar with data encryption of Oracle databases and you need to configure and maintain TDE. If you have questions about TDE, refer to the Oracle documentation.

Restriction: OpenPages supports Oracle TDE only for table spaces. Column-based TDE is not supported.

To implement Oracle TDE, you need to complete two main tasks:

1. Configure a keystore. You can do this step at any time after you install OpenPages.

Your database administrator needs to create a keystore. The steps and requirements for keystores are determined by Oracle. IBM is not responsible for the configuration or maintenance of the keystore.

2. Encrypt the table spaces that support encryption.

To implement Oracle TDE on an existing installation of OpenPages, manual database steps are required. These manual steps require database administrator privileges and skills. If you do not have database administration experience, review these manual steps with a database administrator before you set up Oracle TDE.

A table space can be encrypted only when it is initially created. You cannot alter an existing table space to enable encryption. Instead, you drop the table spaces, re-create them with TDE enabled, and then restore the schema.

Note: Oracle does not support encryption on system, undo, or temporary table spaces.

For more information about TDE, refer to the Oracle documentation, such as the [Oracle Database Advance Security Guide](#).

Prerequisites and process overview

Ensure that your environment meets the prerequisites for Oracle TDE and review the configuration process.

Ensure that your environment meets the following prerequisites:

1. IBM OpenPages with Watson is installed.
2. The Oracle instance is open and accepting connections.
3. All users must be off of the system until all steps in the Oracle TDE configuration process are complete.
4. The database compatibility parameter is set to your version of Oracle:
 - For Oracle 12.2, use 12.2.0
 - For Oracle 18c, use 18.0.0
 - For Oracle 19c, use 19.0.0

Complete the following process to configure Oracle TDE:

1. Configure a software keystore. Refer to the [Oracle documentation](#).
2. Encrypt the OpenPages and Cognos table spaces that support encryption:
 - a. Verify the value of the database compatible parameter.
 - b. Do a full backup of the OpenPages schema.
 - c. Do a full backup of the Cognos schema.
 - d. Shut down all OpenPages components.
 - e. Drop the OpenPages and Cognos table spaces.
 - f. Re-create the OpenPages and Cognos table spaces.
 - g. Verify that the table spaces are encrypted.
 - h. Restore the OpenPages schema.
 - i. Restore the Cognos schema.

Encrypting OpenPages and Cognos table spaces

You can encrypt the OpenPages and Cognos table spaces by using Oracle TDE.

Before you begin

Ensure that no users are on the system before you begin.

Do this procedure after you set up the keystore.

Procedure

1. Log on to the OpenPages database instance as the instance owner.
2. Start SQL*Plus.
3. Verify that the database COMPATIBLE parameter is set to the version of Oracle that you are using.

```
select value from GV$SYSTEM_PARAMETER where name = 'compatible';
```

4. Do a full backup of the OpenPages and Cognos databases.

For more information, see [“Backing up the OpenPages database \(Oracle\)” on page 584](#).

5. Shut down all OpenPages and Cognos components: application servers (admin and non-admin), reporting servers (active and standby), and the search server.

For more information, see [Chapter 25, “Starting and stopping servers,” on page 709](#).

6. Drop all OpenPages and Cognos table spaces.

Do the following steps if your environment meets these criteria:

- OpenPages and Cognos use the same database.
- You are using a standard deployment, where each table space uses a single data file.

If you have multiple data files per table space or if you have customized your deployment in any way, your DBA staff will need to analyze your environment to determine what actions are needed to drop the table spaces.

- a) Determine the list of table spaces.

The default table space names are:

```
AURORA  
INDX  
AURORA_SNP  
AURORA_NL  
AURORA_NLI  
AURORA_CLOB_DATA  
AURORA_DOMAIN_INDX  
CRN
```

Run the following query as a DBA user get a list of the existing table spaces:

```
select tablespace_name from dba_tablespaces;
```

- b) Run the following query to collect information about the table spaces.

You will use this information in a later step.

If you use custom table space names, modify the WHERE clause.

```
select dt.tablespace_name,  
       df.file_name,  
       ceil(df.bytes/1048576) || ' M' as file_size  
  from DBA_TABLESPACES dt,  
       DBA_DATA_FILES df  
 where dt.tablespace_name = df.tablespace_name  
   and dt.tablespace_name in  
     ('AURORA','INDX','AURORA_SNP','AURORA_NL','AURORA_NLI',  
      'AURORA_CLOB_DATA','AURORA_DOMAIN_INDX','CRN');
```

Example output:

TABLESPACE_NAME	FILE_NAME	FILE_SIZE
AURORA	/home/oracle/app/oradata/aurora.dbf	640 M
AURORA_CLOB_DATA	/home/oracle/app/oradata/aurora_clob_data.dbf	128 M
AURORA_DOMAIN_INDX	/home/oracle/app/oradata/aurora_domain_indx.dbf	128 M
AURORA_NL	/home/oracle/app/oradata/aurora_nl.dbf	128 M
AURORA_NLI	/home/oracle/app/oradata/aurora_nli.dbf	128 M
AURORA_SNP	/home/oracle/app/oradata/aurora.snp.dbf	256 M
INDX	/home/oracle/app/oradata/indx.dbf	640 M
CRN	/home/oracle/app/oradata/crn.dbf	512 M



Attention: If a table space name appears twice in the output, the database uses more than one data file per table space. In this case, contact your database administrator before you continue.

- c) Delete the database objects.

Log in to SQL*Plus as the OpenPages database user and run the following script:

```
@AuroraDbDelete.sql
```

When the script completes, log out of SQL*Plus.

- d) Drop the table spaces.

Log in to SQL*Plus as a DBA user and run the following commands. If you use custom table space names, use the names that you found in step 6a.

```
drop tablespace AURORA including contents and datafiles;
drop tablespace INDX including contents and datafiles;
drop tablespace AURORA_SNP including contents and datafiles;
drop tablespace AURORA_NL including contents and datafiles;
drop tablespace AURORA_NLI including contents and datafiles;
drop tablespace AURORA_CLOB_DATA including contents and datafiles;
drop tablespace AURORA_DOMAIN_INDX including contents and datafiles;
drop tablespace CRN including contents and datafiles;
```

7. Re-create the table spaces with Oracle TDE configured.

- a) Create a .sql file that contains the commands.

Copy the following template into a file. Make the following changes to the file:

- If you use custom table space names, replace the table space names with the names from step 6a.
- Replace the placeholders with the values from step 6b.
- Decide which encryption algorithm to use, and uncomment it from the define encrypt_var=' ' list.
- Save the file.

```
----- **** Oracle Transparent Data Encryption ****
-- You can modify the encryption variable below or use one of the provided
-- options. To use a provided option, uncomment the desired algorithm from
-- the list below.

define encrypt_var=''
--define encrypt_var='ENCRYPTION USING ''3DES168''' DEFAULT STORAGE(ENCRYPT)'
--define encrypt_var='ENCRYPTION USING ''AES128''' DEFAULT STORAGE(ENCRYPT)'
--define encrypt_var='ENCRYPTION USING ''AES192''' DEFAULT STORAGE(ENCRYPT)'
--define encrypt_var='ENCRYPTION USING ''AES256''' DEFAULT STORAGE(ENCRYPT)'

create tablespace AURORA datafile '<file name from query>'
  size <file size from query> M reuse autoextend on
  next 128 M &&encrypt_var;

create tablespace INDX datafile '<file name from query>'
  size <file size from query> M reuse autoextend on
  next 128 M &&encrypt_var;
```

```

create tablespace AURORA_SNP datafile '<file name from query>'
  size <file size from query> M reuse autoextend on
  next 128 M &&encrypt_var;

create tablespace AURORA_CLOB_DATA datafile '<file name from query>'
  size <file size from query> M reuse autoextend on
  next 128 M &&encrypt_var;

create tablespace AURORA_DOMAIN_INDX datafile '<file name from query>'
  size <file size from query> M reuse autoextend on
  next 128 M &&encrypt_var;

create tablespace AURORA_NL nologging datafile '<file name from query>'
  size <file size from query> M reuse autoextend on
  next 128 M extent management local uniform size 2 M &&encrypt_var;

create tablespace AURORA_NLI nologging datafile '<file name from query>'
  size <file size from query> M reuse autoextend on
  next 128 M extent management local uniform size 2 M &&encrypt_var;

create tablespace CRN datafile '<file name from query>'
  size <file size from query> M reuse autoextend on
  next 128 M &&encrypt_var;

```

Sample file:

```

-----
-- **** Oracle Transparent Data Encryption ****
-- You can modify the encryption variable below or use one of the provided
-- options. To use a provided option, uncomment the desired algorithm from
-- the list below.
-----
--define encrypt_var=''
--define encrypt_var='ENCRYPTION USING ''3DES168'' DEFAULT STORAGE(ENCRYPT)'
define encrypt_var='ENCRYPTION USING ''AES128'' DEFAULT STORAGE(ENCRYPT)'
--define encrypt_var='ENCRYPTION USING ''AES192'' DEFAULT STORAGE(ENCRYPT)'
--define encrypt_var='ENCRYPTION USING ''AES256'' DEFAULT STORAGE(ENCRYPT)'

create tablespace AURORA datafile
  '/home/oracle/app/oradata/aurora.dbf'
  size 640 M reuse autoextend on next 128 M &&encrypt_var;

create tablespace INDX datafile
  '/home/oracle/app/oradata/indx.dbf'
  size 640 M reuse autoextend on next 128 M &&encrypt_var;

create tablespace AURORA_SNP datafile
  '/home/oracle/app/oradata/aurora.snp.dbf'
  size 256 M reuse autoextend on next 128 M &&encrypt_var;

create tablespace AURORA_CLOB_DATA datafile
  '/home/oracle/app/oradata/aurora_clob_data.dbf'
  size 128 M reuse autoextend on next 128 M &&encrypt_var;

create tablespace AURORA_DOMAIN_INDX datafile
  '/home/oracle/app/oradata/aurora_domain_idx.dbf'
  size 128 M reuse autoextend on next 128 M &&encrypt_var;

create tablespace AURORA_NL nologging datafile
  '/home/oracle/app/oradata/aurora_nl.dbf'
  size 128 M reuse autoextend on next 128 M extent management
  local uniform size 2 M &&encrypt_var;

create tablespace AURORA_NLI nologging datafile
  '/home/oracle/app/oradata/aurora_nli.dbf'
  size 128 M reuse autoextend on next 128 M extent management
  local uniform size 2 M &&encrypt_var;

create tablespace CRN datafile
  '/home/oracle/app/oradata/crn.dbf'
  size 512 M reuse autoextend on next 128 M &&encrypt_var;

```

- b) Log in to SQL*Plus as a DBA user and run the file that you created.

For example, if your file is named `tbsp_create.sql`, log on to SQL*Plus as a DBA user and run the following commands:

```
spool tbsp_create.log
@tbsp_create.sql
exit;
```

8. Grant space privileges to the OpenPages and Cognos users on the new table spaces.

Use the following syntax. If you use custom table space names, replace the table space names with the names from step 6a.

```
alter user <openpages db user> quota unlimited on AURORA;
alter user <openpages db user> quota unlimited on INDX;
alter user <openpages db user> quota unlimited on AURORA_NL;
alter user <openpages db user> quota unlimited on AURORA_NLI;
alter user <openpages db user> quota unlimited on AURORA_SNP;
alter user <openpages db user> quota unlimited on AURORA_CLOB_DATA;
alter user <openpages db user> quota unlimited on AURORA_DOMAIN_INDX;
alter user <cognos db user> quota unlimited on CRN;
```

Example:

```
alter user openpage quota unlimited on AURORA;
alter user openpage quota unlimited on INDX;
alter user openpage quota unlimited on AURORA_NL;
alter user openpage quota unlimited on AURORA_NLI;
alter user openpage quota unlimited on AURORA_SNP;
alter user openpage quota unlimited on AURORA_CLOB_DATA;
alter user openpage quota unlimited on AURORA_DOMAIN_INDX;
alter user cognos quota unlimited on CRN;
```

9. Verify that the table spaces are encrypted.

Log in to the OpenPages database as a DBA user and run the following command. If you use custom table space names, replace the table space names in the WHERE clause with the names from step 6a.

```
select tablespace_name, encrypted, status
  from dba tablespaces
 where tablespace_name in
      ('AURORA', 'INDX', 'AURORA_SNP', 'AURORA_NL', 'AURORA_NLI',
       'AURORA_CLOB_DATA', 'AURORA_DOMAIN_INDX', 'CRN');
```

Verify that the output is similar to the following text:

TABLESPACE_NAME	ENC	STATUS
AURORA	YES	ONLINE
AURORA_CLOB_DATA	YES	ONLINE
AURORA_DOMAIN_INDX	YES	ONLINE
AURORA_NL	YES	ONLINE
AURORA_NLI	YES	ONLINE
AURORA_SNP	YES	ONLINE
INDX	YES	ONLINE
CRN	YES	ONLINE

8 rows selected.

10. Restore the OpenPages schema, and then restore the Cognos schema.

For more information, see [“Import the production data into the test environment” on page 602](#).

11. Restart all OpenPages and Cognos components: application servers (admin and non-admin), reporting servers (active and standby), and the search server.

For more information, see [Chapter 25, “Starting and stopping servers,” on page 709](#).

Shortening the URL for OpenPages with Watson

You can shorten the IBM OpenPages with Watson application URL. You might shorten the URL to support privacy or to support some mobile uses of the URL. To shorten the URL, change the values for properties in various files.

Before you begin

Before you modify the files that are referenced in this procedure, back up the files.

About this task

In the following example of the default and the shortened URL, the port number of the admin application server is 10108:

Default URL

`http://<server_name>:10108/openpages`

Shortened URL

`http://<server_name>:10108/`

Procedure

1. Log on to the admin application server.
2. Stop the Cognos services. For more information, see “[Starting and stopping the Cognos services](#)” on page 717.
3. Edit the following file:
`<OP_HOME>/wlp/usr/servers/<server_name>Server<#/>/configDropins/overrides/op-apps.xml`
4. Look for the following lines:

```
<!-- Specify an alternative context-root here for the primary OpenPages web application -->
<!-- <web-ext id="taskui" moduleName="taskui" context-root="/" />-->
```

5. Uncomment the following line:

```
<web-ext id="taskui" moduleName="taskui" context-root="/" />
```

6. Go to the `<OP_HOME>/aurora/conf/` directory.
7. For each of the properties files that are listed in the following table, open the file in a text editor. Change the current value to the new value, and then save the file:

Table 210. Shorten URL, property values

File name	Current value	New value
aurora.properties	<code>application.url.path=http\://<server_name>:10108/openpages</code>	<code>application.url.path=http\://<server_name>:10108</code>
Server<#>-sosa.properties	<code>application.url.path=http\://<server_name>:10108/openpages</code>	<code>application.url.path=http\://<server_name>:10108</code>
Server<#>-sosa.properties	<code>application.context=/openpages</code>	<code>application.context=</code>

Tip: In a load balanced environment, the `application.url.path` is the fully qualified domain name of the load balancer and its port number.

8. On the Cognos server, navigate to the following folder: `<COGNOS_HOME>/configuration`

- a) Open the `OpenPagesSecurityProvider_OpenPagesSecurityRealm.properties` file in a text editor or XML editor.
 - b) Change the current value to the new value, and then save the file:

Current value
`openpages.application.url=http\://<server_name>\:10108/openpages`

New value
`openpages.application.url=http\://<server_name>\:10108`
9. Restart the OpenPages with Watson application servers. For more information, see “[Starting application servers](#)” on page 709.
 10. Start the Cognos services. For more information, see “[Starting and stopping the Cognos services](#)” on page 717.
 11. After the services are started, log in to OpenPages with Watson.
 12. Click  > **System Configuration** > **Settings**.
 13. Expand the following folders: **Platform** > **Reporting Schema** > **Object URL Generator** > **Detail Page**. Replace the current value with the new value, and then click **Done**.
- Current value**
`/openpages/view.resource.do`
- New value**
`/view.resource.do`
14. Re-create the reporting schema. For more information, see “[Creating or re-creating the reporting schema](#)” on page 120.

Parameters for cluster members

When working with cluster members, there are values for common parameters. You must enter these parameter values consistently across all of the tasks.

For example, a property or code statement requires the name of the machine on which you are adding the cluster member. That value is represented by the `<server_name>` parameter. If the name of the machine on which you are adding the cluster member is `OP_Host`, then you must enter `OP_Host` whenever you are asked to provide the value for `<server_name>`.

Table 211. Parameters for cluster members in IBM WebSphere	
Parameter	Description
<code><OP_HOME></code>	The installation location of the IBM OpenPages with Watson application. By default, <code><OP_HOME></code> is <code>c:\IBM\OpenPages</code> on Windows or <code>/opt/IBM/OpenPages</code> on Linux.
<code><server_name></code>	The hostname of the machine on which you are adding the managed server instance. For example, <code>OP_Host</code>
<code>Server<#></code>	The number of the managed server you are adding to the cluster. For example, If you currently have one managed server on <code>OP_Host</code> , this parameter value would be <code>Server2</code> .
<code><OpenPages_default_server_port #></code>	The value of the <code>op.http.port</code> or <code>op.https.port</code> (if you are using TLS) in the following property file: <code><OP_HOME>/wlp-user/servers/<server_name>Server<#>/bootstrap.properties</code> For example, <code>10108</code>

Configuring HTTP compression in OpenPages with Watson

HTTP compression is a technique used to reduce the network bandwidth that is used to transfer files from the server to the client by compressing web content. Compliant web browsers automatically decompress the content before displaying it to users.

For IBM OpenPages with Watson application servers, HTTP compression is installed during the installation process.

By default, HTTP compression is disabled on the application servers to reduce processor usage and improve performance over a local area network (LAN). On systems that use a router or switch to compresses data, you might also want to disable HTTP compression on both the OpenPages with Watson application and Cognos servers in your environment to avoid double compression.

In situations where clients are primarily accessing the servers by using a narrow network bandwidth (such as modems), enable HTTP compression on both application and Cognos servers.

Note: Files that are already compressed, such as image files, PDF, and .zip files will not be compressed to improve performance.

See these topics for details:

- “[Enabling or disabling HTTP compression on application servers](#)” on page 685
- “[Enabling or disabling compression on the reporting server \(Windows IIS\)](#)” on page 685
- “[Enabling compression on the reporting server \(Apache Web Server\)](#)” on page 686
- “[Disabling compression on the reporting server \(Apache Web Server\)](#)” on page 687

Enabling or disabling HTTP compression on application servers

Follow these steps to enable or disable HTTP compression on IBM OpenPages with Watson application servers via settings in the application user interface.

Note: These steps apply to all OpenPages with Watson application servers in a clustered environment.

Procedure

1. Log on to the OpenPages with Watson application user interface as a user with administrative permissions.
2. Click  > **System Configuration** > **Settings**.
3. Click **Applications** > **Common** > **Configuration**. Change **Show Hidden Settings** to true.
4. Click **Applications** > **Common** > **Configuration** > **HTTP Compression**.
5. Click the **Compression Enabled** setting.
6. In the **Value** box, type one of the following values.
 - **true** – HTTP compression is enabled.
 - **false** - HTTP compression is not enabled.
7. When finished, click **Done**.

The change takes effect immediately.

Enabling or disabling compression on the reporting server (Windows IIS)

You can enable or disable compression on the Cognos server by using Windows IIS.

Procedure

1. On the Cognos server, click **Start** > **Windows Administrative Tools** > **Internet Information Services (IIS) Manager**.

2. In the **Connections** pane:
 - a) Expand **Sites > Default Web Site**.
 - b) Select the name of the Cognos folder (for example, cognos).
3. In **Features View**, under **IIS**:
 - a) Double-click **Compression**.
 - b) Do one of the following:
 - To enable compression, select both **Enable dynamic content compression** and **Enable static content compression**.
 - To disable compression, clear both **Enable dynamic content compression** and **Enable static content compression**.
 - c) In the **Actions** pane, click **Apply**.

Enabling compression on the reporting server (Apache Web Server)

You can enable compression on the Cognos server by using Apache Web Server.

HTTP compression can be enabled or disabled on the Apache Web Server for Windows and Linux environments. The Apache source package includes the mod_deflate module, which provides for the compression of web content. By default, this module is not enabled.

Procedure

1. On the Cognos server, navigate to the `<Apache_Home>/conf` directory.

Where: `<Apache_Home>` is the installation location of the Apache Web Server. For example, for Windows, `C:\Program Files (x86)\Apache2.2` or for Linux, `/opt/pware/`.

2. Navigate to the `httpd.conf` file and do the following:

- a) Make a backup copy of the file before modifying it.
- b) Open the `httpd.conf` file in a text editor of your choice.

3. In the `httpd.conf` file, load the `mod_deflate` module as follows.

- a) Verify that the following statement is present at the beginning of the file:

```
LoadModule deflate_module modules/mod_deflate.so
```

- b) If the `mod_deflate` module statement in Step 3a is commented out (has a # (number sign) at the beginning of the line), then remove the # (number sign) so the compression module will be loaded.

4. At the bottom of the `httpd.conf` file, add the following block of configuration code to enable compression:

```
<IfModule deflate_module>
SetOutputFilter DEFLATE
<IfModule setenvif_module>
# Netscape 4.x has some problems
BrowserMatch ^Mozilla/4 gzip-only-text/html
# Netscape 4.06-4.08 have some more problems
BrowserMatch ^Mozilla/4\.0[678] no-gzip
# MSIE masquerades as Netscape, but it is fine
BrowserMatch \bMSI[E] !no-gzip !gzip-only-text/html
# Don't compress already-compressed files
SetEnvIfNoCase Request_URI \.(?:gif|jpe?g|png)$ no-gzip dont-vary
SetEnvIfNoCase Request_URI \.pdf$ no-gzip dont-vary
SetEnvIfNoCase Request_URI \.(?:exe|t?gz|zip|bz2|sit|rar)$ no-gzip dont-vary
# Make sure proxies don't deliver the wrong content
Header append Vary User-Agent env=!dont-vary
</IfModule>
</IfModule>
```

5. Restart the Apache Web Server:

- For Windows:

- Click **Start > Windows Administrative Tools > Services**.
 - Right-click the Apache<*version*> service and select **Restart**.
 - For Linux:
 - Log on to the Cognos server as the root user.
 - Navigate to the <*Apache_Home*>/bin directory.
 - Enter the following command to stop the server:

```
./apachectl stop
```

 - Type the following command to re-start the server:
- ```
./apachectl start
```

## Disabling compression on the reporting server (Apache Web Server)

You can disable compression on the Cognos server with Apache Web Server.

### Procedure

1. On the Cognos server, navigate to the <*Apache\_Home*>/conf directory.  
Where: <*Apache\_Home*> is the installation location of the Apache Web Server. For example, for Windows, C:\Program Files (x86)\Apache2.2 or for Linux, /opt/pware/.
2. Navigate to the httpd.conf file and do the following:
  - a) Make a backup copy of the file before modifying it.
  - b) Open the httpd.conf file in a text editor of your choice.
3. From the bottom of the httpd.conf file, remove the following block of configuration code to disable compression:

```
<IfModule deflate_module>
SetOutputFilter DEFLATE
<IfModule setenvif_module>
Netscape 4.x has some problems
BrowserMatch ^Mozilla/4 gzip-only-text/html
Netscape 4.06-4.08 have some more problems
BrowserMatch ^Mozilla/4\.0[678] no-gzip
MSIE masquerades as Netscape, but it is fine
BrowserMatch \bMSI[E] !no-gzip !gzip-only-text/html
Don't compress already-compressed files
SetEnvIfNoCase Request_URI \.(?:gif|jpe?g|png)$ no-gzip dont-vary
SetEnvIfNoCase Request_URI \.pdf$ no-gzip dont-vary
SetEnvIfNoCase Request_URI \.(?:exe|t?gz|zip|bz2|sit|rar)$ no-gzip dont-vary
Make sure proxies don't deliver the wrong content
Header append Vary User-Agent env!=dont-vary
</IfModule>
</IfModule>
```

4. When finished, save the file.
5. Restart the Apache Web Server:
  - For Windows:
    - Click **Start > Windows Administrative Tools > Services**.
    - Right-click the Apache<*version*> service and select **Restart**.
  - For Linux:
    - Log on to the Cognos server as the root user.
    - Navigate to the <*Apache\_Home*>/bin directory.
    - Enter the following command to stop the server:

```
./apachectl stop
```

- Type the following command to re-start the server:

```
./apachectl start
```

## Factors that affect performance of views

When you design views, keep in mind the following factors that can affect the performance.

### Number of paths

The more paths in the view the more work the application must do to traverse those paths and provide a result. The more paths that you specify the longer it takes to provide a result.

### Depth of paths

Each object type in the path results in an incremental increase in the work that is required to traverse the path. The deeper a certain path is, the longer it takes to provide a result for that path.

### Number of child objects per top-level object

The ratio of top-level objects to child objects determines how much work the application must do to gather the total result set. The more child objects per top-level object, the longer it takes to provide a result.

### Security rules (RLS/FLS)

Security rules are processed in the context of the individual instance of an object. The inclusion of even a simple security rule increases the work that is required in the application to obtain a result set. As the complexity of the security rule increases, the time it takes to provide a result also increases.

## Server tuning settings

To avoid time-out issues when using IBM OpenPages with Watson, you must configure the servers and the database.

**Important:** All tuning settings assume a maximum of 1,000 concurrent users per node.

## Changing JVM options on application servers

You can adjust the Java Virtual Machine (JVM) options on the IBM OpenPages with Watson application servers.

### About this task

The IBM OpenPages with Watson installation process configures the JVM when you install, upgrade, or migrate OpenPages. You can view the default JVM options in the following file: <OP\_HOME>/wlp-usr/servers/<server\_name>Server<#>/jvm.options. In most cases, you do not need to change the defaults. If you do need to change them, use an override file.

### Procedure

1. Log on to the application server.
2. Edit the following file: <OP\_HOME>/wlp-usr/servers/<server\_name>Server<#>/configDropins/overrides/jvm.options

If the file does not exist, create it by using a text editor.

3. Type the JVM options that you want to change. Type each option on a new line.

For example, the following lines set the initial heap size to 1 GB and the maximum heap size to 4 GB.

```
-Xms1g
-Xmx4g
```

**Note:** This example shows the options that OpenPages uses by default.

For more information, see the WebSphere Liberty documentation.

4. If this is a load-balanced environment, repeat this procedure on each application server in the load-balanced environment.
5. Restart all OpenPages with Watson services.

For more information, see “[Starting application servers](#)” on page 709.

## Configuring the reporting server

Configure the reporting server to avoid time-out issues.

### About this task

You configure the reporting server by using IBM Cognos Configuration and IBM Cognos Administration.

### Procedure

1. Log on to the Cognos server as a user with administrative permissions.
2. Go to the <COGNOS\_HOME>/bin64 directory.
3. Double-click the cogconfigw.exe file to start IBM Cognos Configuration, the IBM Cognos Analytics configuration tool.
4. In the **Explorer** pane, expand **IBM Cognos services**, and click the **IBM Cognos** service.
5. In the properties pane, set the **Maximum memory for Tomcat in MB** property to **1024**.
6. From the **File** menu, click **Save** to save the updated IBM Cognos Analytics configuration.
7. Go to IBM Cognos Administration, click the **Configuration** tab, and then click **Dispatchers and Services**.
8. Click the dispatcher that is used by your IBM Cognos Analytics installation, and in the list of services find **ReportService**.
9. In the **Actions** column, click the **Set properties - ReportService** icon associated with the report service.
10. In the report service properties page, click the **Settings** tab, and specify the following settings.

**Note:** To filter on the tuning settings in the list, under **Category**, click **Tuning**.

- Set the **Number of low affinity connections for the report service during non-peak period** to **8**.
- Set the **Maximum number of processes for the report service during non-peak period** to **8**.
- Set the **Number of low affinity connections for the report service during peak period** to **8**.
- Set the **Maximum number of processes for the report service during peak period** to **12**.

11. Click **OK** to apply the settings.

## Configuring the database (Db2)

Configure the IBM Db2 database to avoid time-out issues.

### Procedure

1. Open the database console running as a Db2 administrator.
2. Set the tuning parameters by using the following command:

```
db2 update db cfg for <DATABASE_NAME> using <VARIABLE> <VALUE>
```

For example, db2 update db cfg for <DATABASE\_NAME> using SELF\_TUNING\_MEM ON

The following table describes the tuning parameter settings to use. Values shown in brackets are informational when the parameter is set to AUTOMATIC. This enables Db2 to control the parameter and reflects the current setting.

*Table 212. Database tuning parameters*

<b>Parameter</b>	<b>Description</b>	<b>Value (default)</b>
SELF_TUNING_MEM	Self tuning memory	ON
DATABASE_MEMORY	Size of database shared memory (4KB)	AUTOMATIC (2683751)
DB_MEM_THRESH	Database memory threshold	10
LOCKLIST	Max storage for lock list (4KB)	AUTOMATIC (82212)
MAXLOCKS	Percentage of lock lists per application	AUTOMATIC (97)
PCKCACHESZ	Package cache size (4KB)	AUTOMATIC (419456)
SHEAPTHRES_SHR	Sort heap threshold for shared sorts (4KB)	AUTOMATIC (63309)
SORTHEAP	Sort list heap (4KB)	AUTOMATIC (12661)
DBHEAP	Database heap (4KB)	AUTOMATIC (5405)
CATALOGCACHE_SZ	Catalog cache size (4KB)	4000
LOGBUFSZ	Log buffer size (4KB)	2560
UTIL_HEAP_SZ	Utilities heap size (4KB)	306174
STMT_HEAP	SQL statement heap (4KB)	AUTOMATIC (51200)
APPLHEAPSZ	Default application heap (4KB)	25600
APPL_MEMORY	Application Memory Size (4KB)	AUTOMATIC (40000)
STAT_HEAP_SZ	Statistics heap size (4KB)	AUTOMATIC (4384)
DLCHKTIME	Interval for checking deadlock (ms)	10000
LOCKTIMEOUT	Lock timeout (sec)	-1
CHNGPGS_THRESH	Changed pages threshold	80
NUM_IOCLEANERS	Number of asynchronous page cleaners	AUTOMATIC (10)
NUM_IOSERVERS	Number of I/O servers	AUTOMATIC (44)
SEQDETECT	Sequential detect flag	YES
DFT_PREFETCH_SZ	Default prefetch size (pages)	AUTOMATIC
TRACKMOD	Track modified pages	NO
	Default number of containers	1
DFT_EXTENT_SZ	Default tablespace extent size (pages)	32
MAXAPPLS	Max number of active applications	300
AVG_APPLS	Average number of active applications	10

Table 212. Database tuning parameters (continued)

Parameter	Description	Value (default)
MAXFILEOP	Max DB files open per application	61440

3. Save your changes.
4. Validate the changes using the following command:

```
db2 get db cfg for <DATABASE_NAME>
```

## Improve the performance of OpenPages application functions on a Db2 server

You can improve the performance of IBM OpenPages with Watson application functions by collecting performance statistics for the IBM Db2 server, and by rebinding OpenPages pl/sql packages.

Examples of application functions include importing instance data using FastMap, importing metadata using ObjectManager, and updating the OpenPages repository using SCOR rules.

Up-to-date statistics are necessary for the proper performance of OpenPages applications that use a Db2 server. You can use a script to force the Db2 server to collect statistics, and by default, rebind all OpenPages pl/sql packages. The script requires all OpenPages application services to stop before it runs. For details on stopping servers, see [Chapter 25, “Starting and stopping servers,” on page 709](#).

You run the script from the primary OpenPages application server. You do not need to run this script from all cluster member servers, but you must stop all cluster member services before running the script to rebind OpenPages pl/sql packages.

If a database is still running, you see the error SQL1026N. If this happens, verify that OpenPages services are not running, and disconnect all active connections to the database before continuing.

1. For Windows users only, type the following command in a command prompt window to initialize the Db2 command line processor (CLP):

```
db2cmd
```

2. Browse to the <OP\_HOME>/aurora/bin/db2stats directory.
3. Run the following script:

- On Windows: CollectSchemaStatistics.bat [-n] [-i]
- On Linux: CollectSchemaStatistics.sh [-n] [-i]

Use these parameters as required:

- [-n] to skip rebinding of database packages.
- [-i] to run the script in interactive mode.

The script execution time varies depending on OpenPages application usage.

You can schedule this script to run by using a task scheduler, cronjob, or similar utility. The suggested schedule to use is as follows:

- Schedule the script to run daily without rebinding of OpenPages pl/sql packages.
- Schedule the script to run once a week with rebinding of OpenPages pl/sql packages.

# Installing tools and utilities (IBM OpenPages with Watson)

---

Tools and utilities, such as ObjectManager, are available on the application servers. But you can also install them on remote systems, such as your laptop, and run them remotely.

## Before you begin

The computer where you install the tools and utilities must meet the following requirements:

- IBM SDK, Java Technology Edition 8 or Java Runtime Environment (JRE) 8 is installed.
- JAVA\_HOME is defined.
- The computer must be able to communicate with the OpenPages application server.

## About this task

Do this task if you want to run any of the following tools from a remote system:

- ObjectManager: See [Chapter 27, “The ObjectManager tool,” on page 731](#).
- Update Password Encryption Algorithm (UPEA): See [“Updating the password encryption algorithm” on page 61](#).
- chng-sys-password.sh | .bat: See [“Changing the OPSystem password” on page 637](#).
- RpsRpf.sh | .bat: A command line tool for creating the reporting schema and generating the reporting framework. See [“Generating the reporting schema and framework from a command line” on page 121](#).
- Notification Manager: See [Appendix A, “The Notification Manager,” on page 925](#).

If you're using IBM OpenPages for IBM Cloud Pak for Data, see [Installing tools and utilities in Cloud Pak for Data](#).

## Procedure

1. Get the installation package.

Go to the /OP\_<version>\_Main/OP\_<version>\_Tools directory on the installation media.  
Download the openpages-tools-client.zip file.

2. Extract the openpages-tools-client.zip file to a new directory.

3. Go to the openpages-tools-client/bin directory.

4. Open the openpages-tools-client.properties file in a text editor.

5. Update the value of the rest.url.path property.

Type the base URL of the public REST API on the application server.

```
https\://<host>\:<port>/grc/api
```

Replace <host> and <port> with the hostname and port of the OpenPages application server.

6. By default, the application server's TLS (SSL) certificate is checked for validity when you run tools such as ObjectManager. To change this behavior, update the insecure.skip.tls.verify property.

For more information, see [“Tools properties and parameters” on page 934](#).

7. Save and close the file.

## Results

You can now run the tools by using the scripts and properties files in the openpages-tools-client/bin directory.

## Using log files

The IBM OpenPages with Watson application writes error and other messaging information to a standard set of log files. You can use these log files to troubleshoot reporting and general user errors that may occur.

## Configuring extended access logging on WebSphere Liberty

You can configure extended access logging on WebSphere Liberty.

### Procedure

1. Log on to the application server.

2. Edit the following file:

<OP\_HOME>/wlp/usr/servers/<server\_name>/configDropins/overrides/op-apps.xml

3. Add the following lines to the file.

```
<httpAccessLogging id="accessLogging"/>
<httpEndpoint id="defaultHttpEndpoint" accessLoggingRef="accessLogging"/>
```

For more information about logging options, see the WebSphere Liberty [documentation](#).

4. Repeat these steps on each application server.

### Results

The log file is <OP\_HOME>/wlp/usr/servers/<server\_name>/logs/http\_access.log.

## Gathering logs with the LogCollector user interface

Use the LogCollector user interface to collect log files and diagnostic data from the IBM OpenPages with Watson environment and from OpenPages databases.

If you prefer to enable trace logging using the auroralogging.properties file, see [Enable trace logging](#).

LogCollector gathers log files into a .zip file that you can download. When your application servers are clustered, a .zip file is available for each application server.

LogCollector doesn't collect Cognos logs or global search logs.

**Important:** You can disallow access to the LogCollector UI by removing the  > **Other** > **Logs** menu item. To remove the menu item, set **Applications** > **Common** > **Administration** > **Enable Manage Logs** to **false**.

This video demonstrates how to collect log files and diagnostic data:

[https://youtu.be/v0-6w\\_MDMj8](https://youtu.be/v0-6w_MDMj8)

### Before you begin

The menu item  > **Other** > **Logs** is visible only to the following users:

- Super Administrators
- Administrators who have the All/SOX/Administration/Logs application permission and access to the **LogCollector Documents** folder. For more information about assigning access control to folders, see *Managing system files and folders* in the *System file management* chapter of the *IBM OpenPages with Watson Administrator's Guide*.

### Procedure

1. Click  > **Other** > **Logs**.

2. Click **Launch**.

The **Launch Log Collector** panel is displayed.

3. If you want to collect log files, set **Log Files** to **True**.

4. If you want to gather database diagnostics, set **Database Diagnostics** to **True**.

5. Click **Add**.

When the Log Collector has gathered the logs, a .zip file that contains the logs is displayed. You can download and decompress this file to view its contents.

6. Optional: If you want to enable tracing logs, click **System tracing options**.

a) Enable the tracing activities that you need by setting them to **On**.

b) Click **Save**.

The next time that you launch LogCollector, the .zip file will contain the trace logs.

## Gathering logs with the log collector tool

You can use the LogCollector tool to collect log files and diagnostic data from the IBM OpenPages with Watson environment and from OpenPages databases.

**Note:** If you're using IBM OpenPages for IBM Cloud Pak for Data, use the IBM Cloud Pak for Data web client to collect log files and diagnostic data.

The LogCollector tool collects log files and diagnostic data on an application server.

In a horizontal cluster environment, run the tool on each application server in your environment.

In a vertical cluster, with multiple application servers that are installed on the same machine, the tool gathers logs from all servers. The tool gathers logs from reporting servers only when they are installed on the same machine as one of the application servers. If the search server is also installed on the same machine, for example in a development environment, the tool also collects the search server logs.

The LogCollector tool is in the <OP\_HOME>/bin directory.

The tool uses the following command options:

**Note:** For all command options, the long name command option uses two hyphens (--), whereas the short name uses only 1 hyphen (-).

**--configuration or -c**

Use to specify a configuration file path.

If you do not include this option, the default is LogCollector.xml.

Using --configuration or -c is optional.

**--database or -d**

Use to collect log and diagnostic data from only the database.

**--file or -f**

Use to collect only log and diagnostic files.

**--location or -l**

Use to specify the path where the output file is stored.

If you specify both -l and -t, use -t for the file name and -l for the path. For example, -l /temp -t test.zip creates /temp/test.zip.

If you don't specify -l, the default location is the directory from which you run the command.

**--property or -p**

Use to set property values.

Using --property or -p is optional. If you do not include this option, the utility automatically retrieves these values from the local configuration. You need to supply these property values only if you want to override the default behavior.

You must include -p for each property that you use. For example, -p DB\_OP\_USER <username> -p DB\_OP\_PASSWORD <password>. You can use the following properties:

<b>Property</b>	<b>Description</b>
<b>DB_OP_USER</b>	The OpenPages database user name.
<b>DB_OP_PASSWORD</b>	<p>The OpenPages database user's password.</p> <p>If the password contains special characters, surround the password in quotation marks:</p> <ul style="list-style-type: none"> <li>• Windows: "password"</li> <li>• Linux: 'password'</li> </ul> <p>For more information, see "<a href="#">Special characters in passwords</a>" on <a href="#">page 5</a>.</p>
<b>DB_TYPE</b>	The database type. This value can be db2 or oracle.
<b>DB_URL</b>	The database JDBC URL.

#### **--target or -t**

Use to specify a target package file.

If you do not include this option, the default is LogCollector\_<timestamp>.zip. Using --target or -t is optional.

#### **--help or -h**

Use to display command help.

### **Example: Getting all information**

1. Log in as the Super Administrator user.
2. Open a command line window.
3. Go to the <OP\_HOME>/bin directory. For example, on Microsoft Windows operating systems, go to C:\IBM\OpenPages\bin. On Linux operating systems, go to /opt/IBM/OpenPages/bin.
4. Enter the following command:

On Microsoft Windows operating systems: LogCollector.cmd

On Linux operating systems: ./LogCollector.sh

The tool generates a package file that is named LogCollector\_<timestamp>.zip in the <OP\_HOME>/bin.

### **Example: Specifying a target package file**

1. Log in as the Super Administrator user.
2. Open a command line window.
3. Go to the <OP\_HOME>/bin directory. For example, on Microsoft Windows operating systems, go to C:\IBM\OpenPages\bin. On Linux operating systems, go to /opt/IBM/OpenPages/bin.
4. Enter the following command:

On Microsoft Windows operating systems: LogCollector.cmd -t LogCollector.zip

On Linux operating systems: ./LogCollector.sh -t LogCollector.zip

The tool generates a package file that is named LogCollector.zip in the <OP\_HOME>/bin directory.

### **Example: Getting information for the database**

1. Log in as the Super Administrator user.
2. Open a command line window.

3. Go to the <OP\_HOME>/bin directory. For example, on Microsoft Windows operating systems, go to C:\IBM\OpenPages\bin. On Linux operating systems, go to /opt/IBM/OpenPages/bin.
4. Enter the following command:

On Microsoft Windows operating systems: LogCollector.cmd -d

On Linux operating systems: LogCollector.sh -d

The tool generates a package file that is named LogCollector\_<timestamp>.zip in the <OP\_HOME>/bin.

## **Example: Getting information from a database and specifying the connection information**

This example shows how to use the -d and -p options. Use -p when you want to override the database connection information that is configured on your local server.

1. Log in as the Super Administrator user.
2. Open a command line window.
3. Go to the <OP\_HOME>/bin directory. For example, on Microsoft Windows operating systems, go to C:\IBM\OpenPages\bin. On Linux operating systems, go to /opt/IBM/OpenPages/bin.
4. Enter the following command:

On Microsoft Windows operating systems:

```
LogCollector.cmd -d -p DB_TYPE db2 -p DB_URL jdbc:db2://localhost:50000/OPX
-p DB_OP_USER openpage -p DB_OP_PASSWORD "password"
```

On Linux operating systems:

```
./LogCollector.sh -d -p DB_TYPE db2 -p DB_URL jdbc:db2://localhost:50000/OPX
-p DB_OP_USER openpage -p DB_OP_PASSWORD 'password'
```

The tool generates a package file that is named LogCollector\_<timestamp>.zip in the <OP\_HOME>/bin.

## **OpenPages with Watson standard log files**

These log files used the Apache Log4j 2 framework. For more information on Apache Log4j 2, see the [Apache Log4j 2 documentation](#).

### **Log files on application servers**

Log files on the application servers contain information to understand what occurs during startup and application usage.

The IBM OpenPages with Watson standard Application Server log files are located in <OP\_Home>/aurora/logs and <OP\_Home>/aurora/logs/debug. File names vary depending on your environment.

Where <server\_name> is the name of the IBM OpenPages with Watson application server.

<#> represents the number of the server (for example, opappServer1).

*Table 213. Application server log files*

<b>This log file...</b>	<b>Contains this type of information...</b>
<server_name>Server<#>-startup.log	Messages written during initialization of the OpenPages with Watson application caches on the OpenPages server.

*Table 213. Application server log files (continued)*

<b>This log file...</b>	<b>Contains this type of information...</b>
<server_name>Server<#>-aurora.log	Errors, exceptions, and informational messages written during OpenPages with Watson application use.
<server_name>Server<#>-reportingframework.log	Logs for the reporting framework

## **Client tool log files**

Client tools are tools that you can run from a remote system. Log files for client tools contain information about errors and exceptions, and also contain informational messages written by OpenPages client tools, such as Notification Manager and ObjectManager.

The IBM OpenPages with Watson client tool log files are located in <OP\_Home>/bin/logs where <OP\_Home> is the folder where you set up the client tools.

*Table 214. Client tool log files*

<b>This log file...</b>	<b>Contains this type of information...</b>
<OP_Home>/bin/logs/openpages-tools-client.log	Messages written for all OpenPages client tools including ObjectManager.
<OP_Home>/bin/logs/ObjectManager.log	Messages written for ObjectManager client commands only.

For more information about client side tools, see [“Installing tools and utilities \(IBM OpenPages with Watson\)” on page 692](#).

## **Changing the size and number of backups of the aurora log file**

An IBM OpenPages with Watson administrator can control the maximum size of the aurora log file and how many backup files are created when the file reaches its maximum size.

### **About this task**

The default maximum file size of the auroralogging.properties is 1024 KB. The default number of backups is 10.

### **Procedure**

1. Log on to the OpenPages application server.
2. Go to <OP\_HOME>/aurora/conf where <OP\_HOME> is the OpenPages installation location.  
By default, <OP\_HOME> is c:\IBM\OpenPages on Windows or /opt/IBM/OpenPages on Linux.
3. Back up the auroralogging.properties file.
4. Open the auroralogging.properties file with a text editor.
5. To change the maximum file size of the auroralogging.properties file, modify the appender.FILE.policies.size.size property.

For example, to change the maximum file size to 5120 KB for all appenders, change the property to the following:

```
appender.FILE.policies.size.size = 5120KB
```

You can define the maximum file size for each appender using the following format:

```
appender.<appender_name>.policies.size.size = <file_size>
```

- To change the number of backups of the auroralogging.properties file, modify the appender.FILE.strategy.max property.

For example, to change the number of backups to 20 for all appenders, change the property to the following:

```
appender.FILE.strategy.max = 20
```

You can define the number of backups for each appender using the following format:

```
appender.<appender_name>.strategy.max = <number_of_backups>
```

## Enabling trace logging

You can enable trace logs for different features within IBM OpenPages with Watson to help you to diagnose issues that you might encounter.

IBM OpenPages with Watson

You can enable trace log options in the following ways:

- Use the LogCollector user interface. For more information, see [Gathering logs with the LogCollector user interface](#).
- Change the auroralogging.properties file. To use this method, follow the steps in this topic.

## About this task

Trace logging generates a large amount of data on the application server. Enable trace logging only during testing and when other users are not on the system. Make sure to disable trace logging before users access the server again.

When trace logging is enabled, separate log files are created in the `<OP_HOME>/aurora/logs/debug` directory. These log files have a suffix that indicates the log type, such as `<server_name>-workflow.log`, and `<server_name>-sdk.log`.

Generally, trace logs contain the following information:

- Enter and exit messages for relevant API calls.
- Timings for each method.
- Targeted debug logging.
- Some appenders also support `apiutilinterceptor` and `apiutilinterceptorresponse` loggers, which log HTTP API requests and responses.

The following trace logs are available:

Table 215. Appenders and associated loggers

Purpose	Appender	Loggers	Log file location
Logs API requests.	api	apimove, apiresource, apischeduler, appservice, resourceutilrespviewrule, toolboxmanager	<code>&lt;OP-HOME&gt;/aurora/logs/debug/&lt;server_name&gt;-api&lt;log_suffix&gt;.log</code>

Table 215. Appenders and associated loggers (continued)

Purpose	Appender	Loggers	Log file location
Applications Common Logger	app-common	addnewappcommon, app-common, dependcommon, relationcommon, sosacommon, taglibcommon, utilcommon	<OP-HOME>/aurora/logs/debug/<server_name>-app-common<log_suffix>.log
Tracks LDAP operations for the LDAP user provisioning.	auth	ldapui, logon, logonerrortag, logonfilter, opappsession, opsession, securityservice, securityutil, sso	<OP-HOME>/aurora/logs/debug/<server_name>-auth<log_suffix>.log
Logs information for debugging the antivirus scanner.	avscanner	avscanner	<OP-HOME>/aurora/logs/debug/<server_name>-avscanner<log_suffix>.log
Logs application-specific cache messages.	cache	auroracache, metadatacache, objectprofilecache, respviewcache, sdkcache	<OP-HOME>/aurora/logs/debug/<server_name>-cache<log_suffix>.log
Logs all calculations.	calculation	calcservice, calculation	<OP-HOME>/aurora/logs/debug/<server_name>-calculation<log_suffix>.log
Logs computed fields, reporting fragments, and connections to IBM Cognos Analytics from OpenPages.	cognos	cognos, cognosreports, cognosservice, reportsservice	<OP-HOME>/aurora/logs/debug/<server_name>-cognos<log_suffix>.log
Logs information specific to IBM Cloud Pak for Data or SaaS operations.	cp4dsaas	cp4dldap, cp4dsecurity, rabbitmq, saasuser	<OP-HOME>/aurora/logs/debug/<server_name>-cp4dsaas<log_suffix>.log
Logs all database Create/Read/Update/Delete operations and associated access data.	dataaccess	dataaccess	<OP-HOME>/aurora/logs/<server_name>-dataaccess<log_suffix>.log

Table 215. Appenders and associated loggers (continued)

Purpose	Appender	Loggers	Log file location
Logs database service operations.	dbquery	dbservice, queryapiservice, queryservice, repositoryservice, resourcemanager	<OP-HOME>/aurora/logs/debug/<server_name>-dbquery<log_suffix>.log
Logs third-party feeds, such as Thomson Reuters or Wolters Kluwer, and Watson Knowledge Catalog integrations.	feeds	feeds, apiutilinterceptor, apiutilinterceptorresponse	<OP-HOME>/aurora/logs/debug/<server_name>-feeds<log_suffix>.log
Logs information for debugging connections to Solr on the search server from the OpenPages application server for Global Search.	globalsearch	globalsearch, searchapi, searchservice	<OP-HOME>/aurora/logs/debug/<server_name>-globalsearch<log_suffix>.log
Logs information for lossevent events.	lossevent	lossevent	<OP-HOME>/aurora/logs/debug/<server_name>-lossevent<log_suffix>.log
Logs machine learning operations to debug issues with machine learning integration.	machinelearning	machinelearning, apiutilinterceptor, apiutilinterceptorresponse	<OP-HOME>/aurora/logs/debug/<server_name>-machinelearning<log_suffix>.log
Logs successful and failed login and logout attempts.	opaccess	opaccess	<OP-HOME>/aurora/logs/<server_name>-opaccess<log_suffix>.log
Logs database access.	persistence	persistence, persistenceroot	<OP-HOME>/aurora/logs/debug/<server_name>-persistence<log_suffix>.log
Logs information for questionnaire operations.	questionnaire	questionnaire, questionnaireservice	<OP-HOME>/aurora/logs/debug/<server_name>-questionnaire<log_suffix>.log

*Table 215. Appenders and associated loggers (continued)*

Purpose	Appender	Loggers	Log file location
Logs debug information for the reporting framework generation.	reportingframework	reportingframework, rps	<OP-HOME>/aurora/logs/<server_name>-reportingframework<log_suffix>.log
Logs access to custom REST API endpoints.	rest	rest, restinterceptor	<OP-HOME>/aurora/logs/debug/<server_name>-rest<log_suffix>.log
Logs REST API information.	restapi	restapi	<OP-HOME>/aurora/logs/debug/<server_name>-restapi<log_suffix>.log
Logs information for debugging the third-party component, named Quartz, which is used by the OpenPages Scheduling service.	scheduler	quartz	<OP-HOME>/aurora/logs/debug/<server_name>-scheduler<log_suffix>.log
Logs information for debugging the OpenPages Scheduler Service.	scheduler	scheduler, schedulerapi	<OP-HOME>/aurora/logs/debug/<server_name>-scheduler<log_suffix>.log
Logs all SDK API calls.	sdk	sdk, sdkinvocation	<OP-HOME>/aurora/logs/debug/<server_name>-sdk<log_suffix>.log
Logs SDK API calls.	sdkgeneral	sdkcomparison, sdkcomputation, sdkobjectprofile, sdkmeta, sdkreg	<OP-HOME>/aurora/logs/debug/<server_name>-sdkgeneral<log_suffix>.log
Logs security encryption operations.	security	securityencrypt	<OP-HOME>/aurora/logs/debug/<server_name>-security<log_suffix>.log

Table 215. Appenders and associated loggers (continued)

Purpose	Appender	Loggers	Log file location
Logs services operations.	services	serviceapp, serviceaudit, servicecommon, servicenps, servicepublish, servicerepo, serviceresource, serviceschema, serviceutil, serviceview	<OP-HOME>/aurora/logs/debug/<server_name>-services<log_suffix>.log
Logs trigger evaluations and executions.	trigger	triggerapi, triggerlifecycle, triggers, triggersdk, triggerutil	<OP-HOME>/aurora/logs/debug/<server_name>-trigger<log_suffix>.log
Logs API requests from the UI.	uiapi	appcontroller, apprestcontroller, basecontroller, componentsfilter, dashboard, modelresource, servicefilter, typescontroller	<OP-HOME>/aurora/logs/debug/<server_name>-uiapi<log_suffix>.log
Logs debugging information for the integration with IBM Watson Language Translator.	watson	watson	<OP-HOME>/aurora/logs/debug/<server_name>-watson<log_suffix>.log
Logs IBM Watson Assistant operations.	watsonother	watsonassistant	<OP-HOME>/aurora/logs/debug/<server_name>-watsonother<log_suffix>.log
Logs Watson classifier operations.	watsonother	watsonclassifier, apiutilinterceptor, apiutilinterceptorresponse	<OP-HOME>/aurora/logs/debug/<server_name>-watsonother<log_suffix>.log
Logs Watson mapping operations.	watsonother	watsonmapping	<OP-HOME>/aurora/logs/debug/<server_name>-watsonother<log_suffix>.log
Logs trace information for the Microsoft Office integration.	webdav	webdav	<OP-HOME>/aurora/logs/debug/<server_name>-webdav<log_suffix>.log

Table 215. Appenders and associated loggers (continued)

Purpose	Appender	Loggers	Log file location
Logs all workflow API calls, model calls, and action evaluations.	workflow	workflow, workflowapi, workflowmodel	<OP-HOME>/aurora/logs/debug/<server_name>-workflow<log_suffix>.log

## Procedure

1. Log on to the OpenPages application server.
2. The auroralogging.properties file is automatically updated by the LogCollector user interface. Before you can edit the auroralogging.properties file manually, you must set **Applications > Common > Administration > Enable Manage Trace Options** to **false**.
3. Go to the <OP\_HOME>/aurora/conf directory.
4. Back up the auroralogging.properties file.
5. Open the auroralogging.properties file with a text editor.
6. To use a trace logger, add the name of the logger to the loggers = entry near the beginning of the file, and add its associated appender to the appenders = entry.

For example, to enable workflows, add the logger and appender as follows:

```
appenders = CONSOLE, FILE, startup, reportingframework, workflow
loggers = startup, reportingframework, rps, workflow
```

7. To enable logging for single sign-on authentication events, add the opappsession, securityutil, sso, authentication, logon loggers to the loggers = entry along with the associated appender auth to appenders = entry as shown in the following example:

```
appenders = CONSOLE, FILE, startup, reportingframework, auth
loggers = startup, reportingframework, rps, opappsession, securityutil, sso, authentication,
logon
```

- a) To increase the logging level from DEBUG to TRACE, do the following steps.



**Attention:** When the logging level is set to TRACE, the log can contain Personal Information (PI) such as usernames and emails.

- i) Locate the following lines:

```
#TRACE level may contain sensitive information such as user names
appender.auth.filter.threshold.type = ThresholdFilter
appender.auth.filter.threshold.level = DEBUG
```

- ii) Change appender.auth.filter.threshold.level = DEBUG to appender.auth.filter.threshold.level = TRACE.

8. Save your changes and close the file.

9. When you finish debugging, disable the loggers.

Restore the backup of the auroralogging.properties file. Or, remove the logger and appender names from the loggers = and appenders = entries in the properties file.

Logging configuration is automatically refreshed in 60 seconds without requiring a server restart.

## Viewing information about background processes

You can view information about background processes in the OpenPages with Watson user interface.

## Before you begin

The menu item  > Other > **Background Processes** is only visible to users who have **API** > **Administration** > **Background Process** > **Get Process Info** application permission.

## Procedure

1. Click  > Other > **Background Processes**.  
The list of background processes is displayed.
2. Optional: If you want to filter the processes, click .
3. Optional: To search on process names and descriptions, click in the **Search** box and enter your search criteria.
4. Optional: To see details about a background process, click the **ID** for the process.
  - a) Click the **Information** tab to see more information such as the **Status**, **Percentage Complete**, **Creation Date**, and a list of **Suboperations**.
  - b) Click the **Log** tab to see the log entries associated with the process.

## Troubleshooting browser issues

---

If you have a problem with a browser, review these topics to determine whether a solution is available.

## Optimizing application performance in Microsoft Edge browsers

To optimize the performance of the IBM OpenPages with Watson application in Microsoft Edge browsers, you can increase the disk space setting for temporary internet files to 200 MB on client machines.

## Procedure

1. From the **Control Panel**, open **Internet Options**.
2. Click the **General** tab.
3. Under **Browsing history**, click **Settings**.
4. In the **Temporary Internet Files and History Settings** box, enter 200 in the disk space box.
5. Restart the browser.

## Setting a session inactivity timeout value

The IBM OpenPages with Watson system will timeout a user session after a set period of browser inactivity.

You can modify the value of the inactivity timeout period for the application server and for the reporting server. In general, the timeout period for the IBM Cognos reporting server should be set to a value greater than the application server timeout period.

In this example, the IBM Cognos server inactivity timeout value is set to 90 minutes, and the application server timeout value is set to 60 minutes. If a user performs various tasks in the OpenPages with Watson application for 45 minutes, then returns to view a report, they will be able to do so without having to log on to the reporting server again. However, if the reporting server has a smaller session inactivity value set, such as 15 minutes, then that same user would be required to log on to the reporting server. By default, the IBM WebSphere Application Server has a 30-minute timeout period. The default timeout period for IBM Cognos is 5400 seconds (equivalent to 90 minutes).

## Setting session inactivity timeout values for application servers

You can set session inactivity timeout values for OpenPages application servers.

If you are using IBM OpenPages for IBM Cloud Pak for Data, see [Setting session inactivity timeout values for application servers in IBM OpenPages for IBM Cloud Pak for Data](#).

### Procedure

1. Prepare your environment.
  - a. Log on to the IBM OpenPages with Watson application server as a user with administrative permissions.
  - b. Stop all OpenPages with Watson services. For more information, see [“Stopping application servers” on page 711](#).
2. Go to the overrides directory.  
`<OP_HOME>/wlp-usr/servers/<server_name>Server<#/>/configDropins/overrides/`  
where `<server_name>` is the name of the application server.
3. In a text editor, open the `op-apps.xml` file and look for the following line:  

```
<httpSession cookieSecure="true" invalidationTimeout="90m"/>
```
4. Set the `invalidationTimeout` parameter to the value in minutes. Save and close the file.
5. Do the following steps:
  - a. Restart all OpenPages with Watson services. For more information, see [“Starting application servers” on page 709](#).
  - b. If this is a load-balanced environment, repeat this procedure for each application server in the load-balanced environment.

### What to do next

Set the timeout period for the IBM Cognos reporting server to a value greater than the application server timeout period. For more information, see [“Setting a session inactivity timeout value” on page 704](#).

## Setting session inactivity timeout values for IBM Cognos

You can set a session inactivity timeout value for the IBM Cognos reporting server.

### Procedure

1. Log on to the IBM Cognos server as a user with administrative permissions.
2. Go to the `<COGNOS_HOME>/bin64` directory.

*Table 216. Installation location of the IBM Cognos reporting server*

Operation system	Installation location
Windows	For example, <code>&lt;COGNOS_HOME&gt;</code> is <code>C:\Program Files\ibm\cognos\analytics</code>
Linux	For example, <code>&lt;COGNOS_HOME&gt;</code> is <code>/opt/ibm/cognos/analytics</code>

3. Double-click the `cogconfig.exe` file to start the IBM Cognos Configuration tool.
4. Expand **Security** and click **Authentication**.
5. Find the **Inactivity timeout in seconds** property and type a new value (in seconds) that is greater than the application server timeout value. For example, you could enter 7200 (equivalent to 120 minutes) if the application server timeout value is set to 90 minutes.

6. Save the configuration changes.
7. Restart the IBM Cognos server.

## Setting the Cognos application firewall for browser security

To prevent URL redirection attacks in Cognos, enable Cognos Application Firewall and configure a host list in Cognos Configuration.

The backURL parameter is a standard (and optional) Cognos URL parameter. This parameter, shown in the following example, can be modified to redirect a user to any site. Therefore, the potential exists for an attacker to also use this parameter to redirect a user to a malicious site where sensitive information could be exposed, such as the user's cookie.

```
https://test.my-company.com/ibmcognos/cgi-bin/cognos.cgi?
b_action=xts.run&m=portal/launch.xts&ui.tool=CognosViewer&ui.action
=xrun&encoding=UTF8 &method=newQuery&backURL=http%3a%2f%2fwww.google.com
&m=qs%2fqqs.xts&cafcontextid=&obj=%2fcontent%2fpackage%5b%40name%3d%270openPages%27%5d
```

The [Cognos documentation](#) indicates that the standard method for performing positive validation of URL input parameters and data is to use the Cognos Application Firewall (CAF). If the data does not match a CAF rule, it is rejected.

The IBM OpenPages with Watson installer enables the Cognos Application Firewall by default.

CAF can be configured with a list of host names, including port numbers and domains that a user can access through the backURL parameter. If a backURL parameter contains a host or a domain name that does not appear in the list, the request is rejected. An error message, similar to the following, is displayed to users who try to access invalid domains or hosts through the backURL parameter:

DPR-ERR-2079 Firewall Security Rejection. Your request was rejected by the security firewall.

The CAF setting has a known issue where enabling the firewall sometimes obscures useful error messages. For example, if a report author developed a report and that report had a logic flaw, a generic firewall error message (as shown previously) is displayed rather than a more useful message containing information about the cause of the actual problem.

Although generic firewall messages are considered a safe way to protect information, this type of nondescript CAF error message can make it more difficult to troubleshoot report authoring issues and certain types of configuration issue.

### Procedure

1. Log on to the reporting server as a user with administrative privileges.
2. Start IBM Cognos Configuration:
  - a) On Windows computers, start a Command Prompt window with the **Run as administrator** option.  
On Linux computers, open a shell.
  - b) Navigate to the <COGNOS\_HOME>/bin64 or <COGNOS\_HOME>/bin directory, where <COGNOS\_HOME> is the installation location of the Cognos application.
  - c) Run the following command:

**Windows:**

cogconfig.bat

**Linux:**

./cogconfig.sh

3. In the **Explorer** window, under **Security**, click **IBM Cognos Application Firewall**.
4. In the **Properties** window, for the **Enable CAF validation** property, set the appropriate values.  
For more information, see the [Cognos documentation](#).

By default, IBM Cognos Application Firewall is enabled.

5. Add host and domain names to the IBM Cognos list of valid names.
6. Save the configuration.

## Browser security issues and running reports

Depending on how browser security is configured on client machines, Cognos reports might not launch successfully from the IBM OpenPages with Watson application user interface.

If a client machine that is using the Microsoft Edge browser is unable to run Cognos reports from the OpenPages application user interface, then do the following in **Control Panel > Internet Options**:

- Add each reporting server to the **Trusted sites** zone on that machine.
- On the **Trusted sites** page, clear the **Require server verification (https:) for all sites in this zone** checkbox.
- Modify the settings of the **Trusted Sites** zone and set the **Enable XSS Filter** property to **Disable**
- Set the security level for the **Trusted sites** zone to **Low**.
- Click the **Custom level properties** for the **Trusted Sites** zone. Under **Downloads**, set **Automatic prompting for file downloads** and **File download** to **Enable**.
- Restart the browser

For information on adding trusted sites to the browser, use the browser documentation.

## Browser locale settings and messaging issues

If a user sets the browser to an unsupported locale, logon and other IBM OpenPages with Watson application messages are displayed only in English.

To ensure proper display of messages in the browser, users must set their browsers to a supported locale. For a list of supported locales, see [Chapter 18, “Localizing text,” on page 443](#).

## Browser errors about Content Security Policy

If you see errors in your browser about Content Security Policy and you use clustered application servers, do the following steps to resolve the issue.

Make a note of the server that is mentioned in the Content Security Policy error message.

Add the application server host and port number to the list of values in the **Platform > Security > Content-Security-Policy** setting. The setting uses the Content Security Policy tool syntax. For more information, see [Content Security Policy](#).

For more information, see [“Configure the HTTP response headers” on page 513](#).

## Browser best practices

An IBM OpenPages with Watson browser session is active until one of three conditions is met.

- The user logs out of the OpenPages with Watson application.
- The session expires.
- The browser instance is closed.

The following are some suggested best practices for enhancing browser security that the users should be aware of:

- Logging off from OpenPages with Watson after they finish their work, and closing the browser window to ensure that no sensitive information is stored in the browser cache.
- Blocking their computers from external use when the users are not physically present - either by keeping their computers on stand-by or by locking their accounts.

- Copying (not clicking) a link to the OpenPages with Watson application from an email and then pasting the link into the address bar of the browser window. After pasting the link, users should validate that the link they just pasted matches the link in the text of the email message.
- Configuration of an inactivity timeout - administrators should set this to a desired security level that is based on commonly known levels of inactivity for their organization. For more information, see “[Setting a session inactivity timeout value](#)” on page 704.
- Configuration of the **Cross-site Scripting Filter** setting to check all HTTP GET requests sent to the OpenPages application server.

# Chapter 25. Starting and stopping servers

You can start and stop the IBM OpenPages with Watson application servers, the database server, the Cognos server, and the search server.

## Starting application servers

You can start IBM OpenPages with Watson in Windows and Linux environments.

In a Windows environment, you can start the OpenPages with Watson application servers by using Microsoft Windows services or by running a script.

In a Linux environment, you run a script to start the OpenPages with Watson application servers.

If you are running OpenPages in a load-balanced environment, you must start the server on the cluster administrator first before starting a cluster member.

## Starting application servers by using Windows services

You can start IBM OpenPages with Watson application servers by using Microsoft Windows services.

### About this task

The OpenPages application service is called <server\_name>Server<#>, where <server\_name> is the name of the application server. You can find the server name in the following locations:

- In the installation app on the application server card
- In the deploy.properties file in the op\_server\_name property.

In a load-balanced environment with vertical cluster members, each vertical cluster is numbered in sequence: <server\_name>Server1, <server\_name>Server2, and so on.

By default, the <server\_name>Server<#> services are configured as Manual (the services do not start upon reboot). You can configure a service to start automatically. In Windows Services, change the service to Automatic.

For the IBM OpenPages with Watson application to run, all of the required Microsoft Windows services must be started and the services of supporting applications must be running.

**Tip:** Alternatively, you can start all application services by using a script. For more information, see “[Starting all application services by running a script \(Windows\)](#)” on page 710.

### Procedure

1. Log on to the application server as a user with administrative privileges.
2. Click **Start > Windows Administrative Tools > Services**.
3. Start each application service in sequence, starting with the <server\_name>Server1 service. Click the service, and then click **Start**.

The **Status** column might show **Running** before the startup process is done. Wait before starting the next application service.

Repeat this step for each application service that you want to start.

4. To set a service to start automatically after a restart, change its **Startup Type** to **Automatic**.
5. If you have horizontal application servers, repeat these steps on each of them.

## Starting all application services by running a script (Windows)

The `StartAllServers.cmd` script, which is included with IBM OpenPages with Watson, starts all OpenPages application services on an application server.

**Note:** This information applies only to Microsoft Windows environments.

### About this task

The script uses the following syntax:

```
StartAllServers.cmd [--clean]
```

The `--clean` option is not necessary for normal operation. IBM OpenPages Support might ask you to use this option when providing an interim fix, or if there is a suspected problem with the cached data. If you use this option, the server will be required to recompute any cached data at the next startup, which might take more time than a restart that reuses cached data.

### Procedure

1. Log on to the OpenPages with Watson application server as a user with administrative privileges or as the OpenPages installation user, `opuser`.
2. Open a Command Prompt window (using the **Run as administrator** option) and do the following:
  - a) Navigate to the `<OP_HOME>\bin` directory.  
Where `<OP_HOME>` is the installation location of the OpenPages with Watson application, for example: `c:\IBM\OpenPages`.
  - b) Run the following command:

```
StartAllServers.cmd
```

The log file is: `<OP_HOME>\wlp-usr\servers\<server_name>\logs\messages.log`

3. If you have horizontal application servers, repeat these steps on each of them.

## Starting all application servers by running a script (Linux)

The `startAllServers.sh` script, which is included with IBM OpenPages with Watson, starts all OpenPages application services on an application server.

**Note:** This information applies only to Linux environments.

### About this task

The script uses the following syntax:

```
./startAllServers.sh [--clean]
```

The `--clean` option is not necessary for normal operation. IBM OpenPages Support might ask you to use this option when providing an interim fix, or if there is a suspected problem with the cached data. If you use this option, the server will be required to recompute any cached data at the next startup, which might take more time than a restart that reuses cached data.

The OpenPages application runs only if all of the services are started and all of the services for all supporting applications are running.

### Procedure

1. Log on to the OpenPages application server as a user with administrative privileges or as the OpenPages installation user, `opuser`.
2. Open a shell window.

3. Go to the <OP\_HOME>/bin directory.

4. Run the following script:

```
./startAllServers.sh
```

The application services on the application server are started.

The log file is: <OP\_HOME>/wlp/usr/servers/<server\_name>/logs/messages.log

5. If you have horizontal application servers, repeat these steps on each of them.

## Determining application readiness

This procedure lets you determine whether the application is ready to be accessed after starting up servers.

### Procedure

1. Open the following log file:

<OP\_HOME>/wlp/usr/servers/<server\_name>/logs/messages.log

Where <server\_name> is the name of the application server.

2. Scroll to the end of the log file and search for the message SRVE0242I: [op-apps] [/grc] [api-rest]: Initialization successful. If this line appears, the server is running in production mode and the application is ready to be accessed.

## Stopping application servers

You can stop IBM OpenPages with Watson application servers in Windows and Linux environments.

Stopping the application server prevents IBM OpenPages with Watson from being accessed.

**Important:** If you are running OpenPages with Watson in a load-balanced environment, stop <server\_name>Server1 last.

## Stopping application servers by using Windows services

You can stop IBM OpenPages with Watson application servers by using Microsoft Windows services.

### About this task

Stopping the application services prevents IBM OpenPages with Watson from being accessed.

**Tip:** Alternatively, you can stop all vertical cluster members on an application server by using a script. For more information, see [“Stopping all application servers in Windows by using a script” on page 711](#).

### Procedure

1. Log on to the application server as a user with administrative privileges.

2. Click **Start > Windows Administrative Tools > Services**.

3. Click the <server\_name>Server<#> service and then click **Stop**. Repeat this step for each application service that you want to stop. If you have horizontal application servers, repeat these steps on each of them.

## Stopping all application servers in Windows by using a script

The StopAllServers.cmd stops all OpenPages application services on an application server. The script stops the services in the proper sequence.

Stopping the application services prevents the OpenPages application from being accessed.

## Procedure

1. Log on to the OpenPages with Watson application server as a user with administrative privileges.
2. Launch a Command Prompt window (using the **Run as administrator** option).
3. Navigate to the <OP\_HOME>\bin directory.
4. Run the following command:

```
StopAllServers.cmd
```

5. If you have horizontal application servers, repeat these steps on each of them.

## Stopping all application servers on Linux by using a script

The stopAllServers.sh script stops all OpenPages application services on an application server. The script stops the application services in the proper sequence.

Stopping the application services prevents the OpenPages application from being accessed.

## Procedure

1. Log on to the OpenPages with Watson application server as a user with administrative privileges.
2. Open a shell window and navigate to the <OP\_HOME>/bin directory.
3. Run the following command:

```
./stopAllServers.sh
```

The application services on the application server are stopped.

4. If you have horizontal application servers, repeat these steps on each of them.

## Start or stop the global search services

You can start and stop the global search services by using operating system services or by using scripts.

**Note:** Do not combine the two methods. If you start global search as a Microsoft Windows service, for example, stop global search by stopping the Windows service.

## Starting the global search services by using a script

You can start the global search services by running a script from a command line.

### Before you begin

On the Windows operating system, disable the Microsoft Windows service that is called **IBM OpenPages GRC - Global Search**, if it is enabled. Otherwise, the StartSearchServers.cmd script interferes with the Windows services.

Make sure that the database server is reachable and is running. Otherwise, the search services will not connect and will not start.

## Procedure

1. Start the search services:

- For Windows, at a command prompt enter the following commands:

```
cd <SEARCH_HOME>\opsearchtools\
StartSearchServers.cmd
```

- For Linux, at a command line, enter the following commands:

```
cd <SEARCH_HOME>/opsearchtools/
./StartSearchServers.sh
```

2. Open a browser and point to your search server at ports 8983 and 8985. Make sure that the Solr search platform can be reached.

For example, `http://<search-server>:8983/` and `http://<search-server>:8985/`.

If the verification fails, repeat the preceding step.

3. Log on to IBM OpenPages with Watson as an administrator.

4. Click  > **System Configuration** > **Global Search** and click **Enable**.

## Stopping the global search services by using a script

You can stop the global search services by running a script from a command line.

### Before you begin

On the Windows operating system, disable the Microsoft Windows service that is called **IBM OpenPages GRC - Global Search**, if it is enabled. Otherwise, the `StopSearchServers.cmd` script interferes with the Windows services.

### Procedure

1. Log on to IBM OpenPages with Watson as an administrator.

2. Click  > **System Configuration** > **Global Search** and click **Disable**.

3. Stop the search services:

- For Windows, at a command prompt, enter the following commands:

```
cd <SEARCH_HOME>\opsearchtools\
StopSearchServers.cmd
```

- For Linux, at a command line, enter the following commands:

```
cd <SEARCH_HOME>/opsearchtools/
./StopSearchServers.sh
```

4. For either Windows or Linux, verify that global search is fully stopped.

a) In the directory `<SEARCH_HOME>/opsearchtools/`, examine the files `opsearchtool_openpages.state` and `opsearchtool_folderacl.state` and verify that the PID value is -1.

b) Open a browser and point to your search server at ports 8983 and 8985. Make sure that the Solr search platform cannot be reached.

For example, `http://<search-server>:8983/` and `http://<search-server>:8985/`.

If the stop verification fails, repeat the preceding step and then follow the steps in “[Forcing a reset of global search](#)” on page 943.

## Starting the global search services on Windows

You can start global search as a Microsoft Windows service. The service is called **IBM OpenPages GRC - Global Search**.

### About this task

By default, the service is set to start manually, but you can change the service to start automatically.

**Note:** Make sure that the database server is reachable and is up and running. Otherwise, the search services will not connect and will not start.

## Procedure

1. Log on to the search server as a user with administrative privileges.
2. Click **Start > Windows Administrative Tools > Services**.
3. Locate the service that is called **IBM OpenPages GRC - Global Search**.
4. Click **Start**.
5. If you want the service to start automatically when Windows starts, change the **Startup Type** to **Automatic**.
6. Open a browser and point to your search server at ports 8983 and 8985. Make sure that the Solr search platform can be reached.  
For example, `http://<search-server>:8983/` and `http://<search-server>:8985/`.  
If the verification fails, repeat the preceding step.
7. Log on to IBM OpenPages with Watson as an administrator.
8. Click  **System Configuration > Global Search** and click **Enable**.

## Starting the global search services on Linux

You can start global search as a service.

### About this task

Use the steps in this topic as a guide. Depending on your environment and organization policies, you might decide to use a different method to set up the search service. If you want to use a different method, open the `openpages-search` file and check the commands, and the order of the commands. Modify the commands to meet the needs of your environment.

**Note:** Make sure that the database server is reachable and is up and running. Otherwise, the search services will not connect and will not start.

## Procedure

1. Log on to the search server.
2. Open a shell as the root user.
3. Copy the `<SEARCH_HOME>/opsearchtools/openpages-search` file to the `/etc/init.d/` directory.
4. Copy the `<SEARCH_HOME>/opsearchtools/openpages-search-cfg` file to the `/etc/sysconfig/` directory.
5. Set the execution permission on the `openpages-search` file by running the following command:  
`chmod +x /etc/init.d/openpages-search`
6. If you want the service to start automatically when the system restarts, run the following commands:

```
chkconfig --add openpages-search
chkconfig openpages-search on
service openpages-search start
```

7. Start the global search services by running the following command: `service openpages-search start`
8. Open a browser and point to your search server at ports 8983 and 8985. Make sure that the Solr search platform can be reached.  
For example, `http://<search-server>:8983/` and `http://<search-server>:8985/`.  
If the verification fails, repeat the preceding step.
9. Log on to IBM OpenPages with Watson as an administrator.
10. Click  **System Configuration > Global Search** and click **Enable**.

## Stopping the global search services

If global search is running as a service, you can use the operating system to stop the global search services.

### About this task

If you used the `StartSearchServers.sh|.cmd` script to start the global search services, use the `StopSearchServers.sh|.cmd` script to stop the services. For more information, see [“Stopping the global search services by using a script” on page 713](#).

### Procedure

1. Log on to IBM OpenPages with Watson as an administrator.
2. Click  > **System Configuration** > **Global Search** and click **Disable**.
3. Log on to the search server as a user with administrative privileges.
4. Stop the search services.

Windows

:

- a) Click **Start** > **Windows Administrative Tools** > **Services**.
- b) Locate the service that is called **IBM OpenPages GRC - Global Search**.
- c) Click **Stop**.

On Linux, run the following command:

```
service openpages-search stop
```

5. Verify that global search is fully stopped.
  - a) In the directory `<SEARCH_HOME>/opsearchtools/`, examine the files `opsearchtool_openpages.state` and `opsearchtool_folderacl.state` and verify that the PID value is -1.
  - b) Open a browser and point to your search server at ports 8983 and 8985. Make sure that the Solr search platform cannot be reached.  
For example, `http://<search-server>:8983/` and `http://<search-server>:8985/`.  
If the stop verification fails, repeat the preceding step and then follow the steps in [“Forcing a reset of global search” on page 943](#).

## Start or stop the database services

You can start and stop the database services.

For more information, see the documentation that is provided with your database server:

### IBM Db2

[Managing instances](#)

### Oracle

[Starting Up and Shutting Down](#)

For examples, see [“Starting and stopping the Oracle database server in a Windows environment” on page 715](#) or [“Starting and stopping the Oracle database server in Linux environments” on page 716](#).

## Starting and stopping the Oracle database server in a Windows environment

The following steps show an example of how to start or stop an Oracle database server by using Windows services.

## About this task

For more information, see the Oracle documentation.

Table 217. Oracle services for OpenPages on Windows	
Service Name	Description
Oracle<ORACLE_HOME>TNSListener	Runs the Oracle Database listener service that connects the user to the Oracle database instance.
OracleService<SID>	Used to start and stop the Oracle database instance. Where <SID> represents the database instance identifier, for example OP.
OracleVssWriter<SID>	Where <SID> represents the database instance identifier, for example OP.

## Procedure

1. Log on to the database server as a user with administrative privileges.
2. Click **Start > Windows Administrative Tools > Services**.
3. For each database service listed in Table 217 on page 716, do the following:
  - To start the server, right-click the service name and select **Start**.
  - To stop the server, right-click the service name and select **Stop**.

## Starting and stopping the Oracle database server in Linux environments

The following steps show an example of how to start or stop an Oracle database.

For more information, see the Oracle documentation.

## Procedure

1. Log on to the database server as a user with administrative privileges.
2. In a shell window, navigate to the following directory:

```
<ORACLE_HOME>/bin
```

For example: /opt/oracle/app/product/19.3.0/dbhome\_1/bin.

3. To start Oracle, do the following steps.

- a) Log in to SQL\*Plus.

```
sqlplus / as sysdba
```

- b) Run the following command to start Oracle.

```
startup
```

4. To stop Oracle, do the following steps.

- a) Log in to SQL\*Plus.

```
sqlplus / as sysdba
```

- b) Run the following command to stop Oracle.

```
stop immediate
```

## Starting and stopping the Cognos services

---

You can use the following procedures to start or stop the Cognos services.

These procedures are:

- [“Using the IBM Cognos configuration tool to start and stop the IBM Cognos service” on page 717](#)
- [“Using the Windows operating system to start and stop the IBM Cognos service” on page 717](#)
- [“Using the Linux operating system to start and stop the IBM Cognos service” on page 718](#)

## Using the IBM Cognos configuration tool to start and stop the IBM Cognos service

You can use the IBM Cognos Configuration tool to start or stop the IBM Cognos service.

The IBM Cognos Configuration tool displays the status of the start-up, which can be helpful with troubleshooting.

### Procedure

1. Log on to the reporting server as a user with administrative privileges.
2. Start the IBM Cognos Configuration tool as follows:
  - a) Open a command prompt (using the **Run as administrator** option), or a Linux shell, and navigate to the <COGNOS\_HOME>/bin directory.  
    <COGNOS\_HOME> represents the installation location of the Cognos application.
  - b) Run one of the following commands to open the tool:  
**Windows**  
    cogconfig.bat  
**Linux**  
    ./cogconfig.sh
3. Do one of the following:
  - To start the server, click **Actions > Start**. It might take several minutes for the service to start the first time.  
    If the **Start** option is not available, the service has already started.
  - To stop the service, click **Actions > Stop**.

## Using the Windows operating system to start and stop the IBM Cognos service

Use the following steps to start or stop the IBM Cognos service in a Windows environment using Windows Services.

### Procedure

1. Log on to the reporting server as a user with administrative privileges.
2. Click **Start > Windows Administrative Tools > Services**.
3. Do one of the following:
  - To start the server, right-click the IBM Cognos service and select **Start**.
  - To stop the server, right-click the IBM Cognos service and select **Stop**.

## **Using the Linux operating system to start and stop the IBM Cognos service**

Use the following steps to start or stop the IBM Cognos service in a Linux environment using command-line scripts.

### **Procedure**

1. Log on to the reporting server as a non-root user with administrative privileges.
2. Open a shell window and navigate to the <COGNOS\_HOME>/bin64 directory  
Where <COGNOS\_HOME> is the installation location of the Cognos application.
3. Do one of the following:
  - To start the service, enter the following command: ./cogconfig.sh -s
  - To stop the service, enter the following command: ./cogconfig.sh -stop

# Chapter 26. Migrating OpenPages environments

If your organization has multiple OpenPages environments, you can migrate both the configuration information and the metadata from one environment to another. Migration means exporting from a source environment and importing into a target environment.

You can use the **Export Configuration** tool to create a migration file, which can then be imported by using the **Import Configuration** tool. You can also use **Import Configuration** to import files in XML format. For more information, see “[Supported migration items](#)” on page 720.

**Tip:** You can also use ObjectManager, a command-line interface (CLI) tool, to migrate configuration changes. For more information, see [Chapter 27, “The ObjectManager tool,” on page 731](#).

An OpenPages environment is a set of OpenPages servers that target a single database instance, inclusive of that database instance. For example, your organization might have Development, UAT, and Production environments.

The environment from which you want to export data is referred to as the *source* and the environment into which you want to import data is referred to as the *target*.

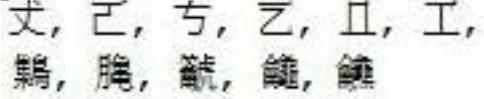
The source and target environments must have the same version and patch level of OpenPages.

## Settings that apply to environment migration

The environment migration settings are found in the **Applications > GRCM > Environment Migration** folder hierarchy.

For instructions on accessing the settings page, see [Chapter 20, “Viewing the Configuration and Settings page,” on page 473](#).

**Tip:** To author an XML settings path, add the OpenPages folder at the beginning of the path. For example: /OpenPages/Applications/GRCM/Environment\_Migration/

Table 218. Environment migration settings	
Setting	Definition
Export File Name Prefix	<p>Prefix to be added to the environment migration export file name. The default prefix, openpages, is used if no value is given. Prefix length is limited to 15 characters. If the prefix is longer than 15 characters, it is truncated.</p> <p><b>Important:</b></p> <ul style="list-style-type: none"><li>The following characters cannot be used in the prefix: ＼ /   * : { } [ ] " ?</li><li>Do not use the special characters as defined in CJK Compatibility Ideographs Unicode Block Name and the four-byte characters as defined in the CJK Unified Ideographs EXTENSION-B Unicode Block Name in the prefix.</li></ul> <p>The special characters to avoid are:</p> 
Special Character Validation	Specifies whether special characters are checked while validating names of metadata. The default is <b>true</b> .

The **ImportConfiguration** and **ExportConfiguration** application permissions are required to access environment migration for import and export. For details on these permissions, see “[Types of application permissions](#)” on page 52.

You must also have read and write permissions on the **Migration Documents** folder. You can see the folder by clicking  > **System Configuration** > **System Files**.

You might also need read and write permissions on other folders, depending on what you are importing and exporting.

For an overview of environment migration, see [Chapter 26, “Migrating OpenPages environments,” on page 719](#).

## Supported migration items

---

You can use the environment migration capability to move items between any two OpenPages environments that are using the same version and patch level of OpenPages.

The following information types are part of environment migration and, as such, you can export them by using **Export Configuration** and import them by using **Import Configuration**.

- Application Text
- Calculations (calculation definitions in GRC Calculations)
- Date Dimension Types
- Date Dimension Type Associations
- Dependent Picklists
- Error Text
- Field Definitions
- Field Dependencies
- Field Groups
- Filters
- Groups/Users (Selecting a group exports the group hierarchy under the group, including sub-groups, users, user and group profile associations, and the group's administrators.)
- Jobs (schedule definitions in the Scheduler)
- Object Profiles
- Object Text
- Object Types
- Object Type Dimensions
- Object Type Relationships
- Recursive Object Levels
- Role Assignments
- Role Templates
- Rule Sets
- Rules (for IBM OpenPages Regulatory Compliance Management)
- Security Rules
- Settings
- Solutions
- Tags

**Note:** Solutions from pre-8.2 environments are displayed with - Legacy in the solution name, for example ORM-Legacy.

- Themes
- Views
- Workflows (workflow definitions in GRC Workflow)

The following supplemental information types can be exported by using ObjectManager and imported in XML format by using **Import Configuration**:

- System data (typically loaded during installation)
  - File types (for example, pptx, xlsx, docx)
  - Application permissions
  - Currencies
  - Reporting folders (channels)
  - Locales
- Instance data
  - Instance data (for example, risk and control objects and field values)
  - Parent and child relationships
- Other
  - Currency exchange rates

**Important:** You must use ObjectManager rather than the environment migration tools in the user interface when you migrate field groups that contain four-byte characters as defined in the CJK Unified Ideographs EXTENSION-B Unicode Block Name, such as:

For information about ObjectManager, see [Chapter 27, “The ObjectManager tool,” on page 731](#).

## Migration files

The environment migration export process creates a file in the Java archive (JAR) format (referred to as a migration file in this documentation). The migration file is saved automatically to the repository.

The exported migration file is named in the `<export file name prefix>-env-mig-<MMddYYkkmmss>` format; where:

- `<export file name prefix>` is the value of the **Export File Name Prefix** setting (see [“Settings that apply to environment migration” on page 719](#)), truncated if the prefix exceeds 15 characters;
- `<MMddYYkkmmss>` represents the month (MM), the day (dd), the year (YY), hour (kk), minute (mm), and seconds (ss) when the export was started.

For example, `openpages-env-mig-011723031416`.

## Display types for fields

When you export fields by using ObjectManager or Environment Migration, the display type is included in the export.

For example, when you export a user/group field, the XML file includes `displayType`, such as:

```
<displayType name="Multi Valued User Selector" ...>
```

If a field exists in a target system, you can update its display type by importing the field. You do not need to import the profiles that use the field. In the XML file, you can specify the `displayType` of the field or leave `displayType` out. If you don't specify a `displayType` in the field definition, the `displayType` from the profile is used.

If a field does not exist in a target system, in addition to importing the field, you must import at least one object type and one profile that use the field. Otherwise, you will need to update the display type manually in the user interface.

## Exporting dependencies

When you export certain configuration items, the export process automatically determines if there are any dependencies required by the configuration items and adds those dependencies to the migration file.

The dependencies that are exported for each type of item are listed in the following table.

Table 219. Dependent items exported	
Item	These dependencies are exported
Object profile	<ul style="list-style-type: none"><li>views</li><li>object types (including all object type dependencies)</li><li>field groups (including all field group dependencies)</li><li>view labels</li><li>dashboards</li></ul>
Object type	<ul style="list-style-type: none"><li>field groups (including any underlying fields)</li><li>field dependencies</li><li>dependent picklists</li><li>public filters</li><li>root folders</li><li>object type images</li><li>corresponding settings and object strings</li><li>object type relationships</li><li>file types (if the object type is file-upload based)</li></ul>
Field group	Any underlying fields
Groups	Exporting a group also exports the subgroups, users, group memberships, profile associations, and group administrators.
Application strings	Any corresponding string keys
Object type dimensions	Any recursive object levels, if associated
Date dimension type associations	Any corresponding date dimension types

## Items that are not migrated

The following items are not exported by the environment migration tools. These items are not available for import into a target environment and the validation process does not identify these items as missing.

If any of the items that you plan to migrate has a dependency on one or more of these items, you need to move the dependent item or items manually prior to using the environment migration tools. For help determining if any dependencies will not be migrated and how to move those dependencies manually, contact IBM OpenPages Support.

## Configuration settings that are not migrated

The configuration settings listed in [Table 220 on page 723](#), are not migrated by the environment migration tools.

**Important:** Do not change the security model with the **Settings > Common > Security > Model** setting on the source system if there is instance data in the target system. If you do, the configuration settings import will fail.

**Note:** If the **Show Hidden Settings** setting is set to false, hidden settings are not migrated. For more information, see [“Show hidden settings” on page 479](#). To migrate hidden settings, set the **Show Hidden Settings** setting to true.

For example, if you export all settings, the settings in this table are not included in the exported JAR file.

Table 220. Configuration settings that are not exported	
Setting description	Location
Mail server name	<b>Applications &gt; Common &gt; Email &gt; Mail Server</b>
SMTP user name	<b>Applications &gt; Common &gt; Email &gt; SMTP User Name</b>
SMTP password	<b>Applications &gt; Common &gt; Email &gt; SMTP Password</b>
SMTP security type	<b>Applications &gt; Common &gt; Email &gt; SMTP Security Type</b>
SMTP port number	<b>Applications &gt; Common &gt; Email &gt; SMTP Port</b>
SOCKS Proxy private IP address	<b>Applications &gt; Common &gt; Email &gt; SOCKS Proxy Private IP Address</b>
Guest password on server	<b>Platform &gt; Application Server Guest Password</b>
JMS listener URLs for all paired servers	<b>Platform &gt; Global Caches &gt; JMS &gt; Listener URLs</b>
Default OpenPages email sender address	<b>Platform &gt; Publishing &gt; Mail &gt; From Address</b>
Default OpenPages email server	<b>Platform &gt; Publishing &gt; Mail &gt; Host</b>
Default OpenPages email username	<b>Platform &gt; Publishing &gt; Mail &gt; Username</b>
OpenPages detail page name for reference by reporting tool	<b>Platform &gt; Reporting Schema &gt; Object URL Generator &gt; Detail Page</b>
OpenPages server name for reference by reporting tool	<b>Platform &gt; Reporting Schema &gt; Object URL Generator &gt; Host</b>
OpenPages server port for reference by reporting tool	<b>Platform &gt; Reporting Schema &gt; Object URL Generator &gt; Port</b>
OpenPages application protocol for reference by reporting tool	<b>Platform &gt; Reporting Schema &gt; Object URL Generator &gt; Protocol</b>
Export File Name Prefix	<b>Applications &gt; GRCM &gt; Environment Migration &gt; Export File Name Prefix</b>
Index search server URL	<b>Platform &gt; Search &gt; Index &gt; Search Server URL</b>
Request search server URL	<b>Platform &gt; Search &gt; Request &gt; Search Server URL</b>
Search server administration URL	<b>Platform &gt; Search &gt; Admin &gt; Search Server Administration URL</b>
Solr user ID	<b>Platform &gt; Search &gt; Solr User ID</b>

Table 220. Configuration settings that are not exported (continued)

Setting description	Location
Solr password	Platform > Search > Solr Password

## Metadata items not migrated

The following metadata items are not migrated by the environment migration tools. If any of these items is not in the target environment, you need to move it manually.

- Triggers
- Custom query subjects
- JSPs
- Instance data

Although instance data is not part of the environment migration JAR files, you can migrate it by exporting it with ObjectManager and then importing the XML file with **Import Configuration**.

For the other items, such as JSPs, you need to copy the files from one environment to the other.

## Security domains are not migrated

Security domains are based on instance data, typically the Business Entity hierarchy. Any instance data can be migrated between systems by using FastMap. Security domains are not migrated by the environment migration tools.

If your system has profiles that contain user fields that are scoped to specific security domain groups, verify that the target environment has all the security domain groups that are referenced by the profiles. If not, configure the target environment to match the source.

For profiles, the import validation process stops the import if any required security domain group is not present in the target environment. An error in the following format is displayed in the validation log:

```
<line#> Processing 'displayTypePropertyValue', Attribute: 'name', Value:
'<group Name>' is not defined in the migration package or in the target
system!: Group Missing!
```

Similarly, if you're migrating role assignments, verify that the target environment has all of the security domain groups that are referenced by the role assignments. If a security domain group is missing, an error message in the following format is displayed in the import log:

```
VALIDATION ERROR: 'businessUnit "<business_entity_path> does not exist.''
```

User fields can have a scope defined that filters the amount of returned search data. This scope definition is based on security domain groups. However, these security domain groups are not migrated by the environment migration tools. If a user field has a scope defined in the source environment, but that configuration does not exist in the target environment, the import will be stopped.

## Reports not migrated

Reports are not migrated by the environment migration tools.

If a profile contains an embedded report that is not available in the target environment, a user with that profile sees a message in the OpenPages with Watson interface that the report is missing.

**Important:** If you want a user to access an embedded report that is not present in the target environment, you must move the report manually from the source environment to the target environment before migrating the environment.

## Item dependencies not migrated by default

Environment migration automatically determines if there are any dependencies required by the exported items and adds those dependencies to the migration file.

However, some items that can be exported for migration are not included automatically as dependencies.

The following metadata items are not exported as a dependency:

- Namespaces

If a profile includes a computed field that relies on a namespace, and that namespace does not exist (or is defined differently) in the target environment, the profile passes import validation. However, a user will not be able to access the computed field in the target environment. To avoid this scenario, ensure that all namespaces upon which computed fields have a dependency are included in the migration file.

- Objects, field groups, and fields

If a filter includes criteria that rely on an object, a field group, or a field that is not already in the target environment, the migration fails. To avoid this scenario, ensure that all objects, field groups, and fields upon which filters have a dependency are included in the migration file.

- Roles and role assignments

When you export role assignments, the export does not include the role templates, users, groups, or the security domains. When you export role assignments, you can also export the role templates, users, and groups. You can migrate security domains by using FastMap.

- Workflows that are used in rules

When you export rules that you created in the **Rules Engine**, the export does not include the workflows that the rules trigger. For example, suppose you have a rule that is called Change Notification that triggers the Send Email Notification workflow. When you export rules, the Send Email Notification workflow is not included in the export. To migrate rules, you need to migrate both rules and their workflows to the target environment.

- Job dependencies

When you export jobs, the export does not include any dependencies, such as workflows or Java classes that the jobs trigger. For example, suppose you have a job that runs the BC Plan Review and Approval workflow. When you export the job, the workflow is not included in the export. To migrate jobs, you need to migrate both jobs and their workflows or Java classes to the target environment.

- Workflow dependencies

When you export workflows, the export does not include dependencies, such as views, object types, and custom actions. To migrate workflows, you need to migrate the workflows and their dependencies to the target environment. For more information, see [“Exporting and importing workflow definitions” on page 432](#).

- Calculation dependencies

When you export calculations, the export does not include any dependencies. To migrate calculations, you need to migrate the calculations and their dependencies to the target environment.

## Environment migration best practices

When you use environment migration to move metadata and configuration items from one environment to another, use the following best practice guidelines to help ensure a smooth transition of information:

- A setting cannot be imported if the target system does not have the dependencies specified in the setting's value. To migrate the setting, first migrate the dependencies (such as object types, field groups, and recursive object levels) without the setting. Then, migrate the setting by using a separate migration file.
- Before you import security rules, you must import the metadata and create the reporting schema in the target environment.

- Before you import users, groups, or role assignments, you must import the security domains (business entities) to the target environment. See “[Items that are not migrated](#)” on page 722. You can use FastMap to export and import business entities.
- Import configuration items during planned downtime, when end users are not accessing that environment. Issues can arise if an end user is working with an item while that item is being imported.
- Replicate the metadata in your production environment to the development and/or test environment where you will be making and testing configuration changes.

Using the same configuration data in all environments ensures that:

- All environments operate on the same baseline set of OpenPages metadata as a starting point.
- Any test configurations or items in a test or development environment are removed, preventing those items from being migrated inadvertently to the production environment.

For more information about replicating environments, see “[The OPBackup utility \(Db2\)](#)” on page 548 or “[The OPBackup utility \(Oracle\)](#)” on page 581.

- Make modifications and additions to configuration items in a test or development environment. After the items are tested, migrate the items to the production environment.
- If you are importing an XML file, you must use the ObjectManager loader file naming convention:

```
<loader-file-prefix>-op-config.xml
```

For more information about the naming convention, see “[Working with loader files](#)” on page 731.

- Before you import configuration items, validate the migration file. See “[Validating a migration file](#)” on page 728.
- If a background import, export, or validate configuration process is currently running on the system, you must wait until processing is complete before you submit another configuration job.
- If you migrate filters for large text fields, you must enable the text feature in your target database so that large text fields display correctly in the filters.

For more information about enabling the IBM Db2 Text Search feature, see “[Enable Db2 text search](#)” on page 567.

For more information about enabling the Oracle Text feature, see “[Enabling Oracle Text](#)” on page 612.

- When you import calculations, the import might fail if your target environment has calculation definitions. The issue occurs when there are input or output field conflicts on an object type. To resolve the issue, disable the existing calculations in your target environment, and then import the calculations again.

## The environment migration process

From a single client system, you can use the OpenPages application to select and export changed configuration items in an OpenPages environment (the source), and then import them into another environment (the target). The environment migration import process automatically validates the imported items to ensure they will work properly in the target environment.

Table 221 on page 726 outlines the process for migrating configuration items from a source environment to a target environment by using the environment migration tools.

Table 221. Tasks for migrating items by using Environment Migration	
Use this environment...	To do this task...
Source	Export the configuration items into a migration file. See “ <a href="#">Exporting configuration items from the source environment</a> ” on page 727.
Target	Import the configuration items into the target environment. See “ <a href="#">Importing configuration items to the target environment</a> ” on page 727.

This video demonstrates how to migrate your system configuration:

<https://youtu.be/4uO3O8srqIY>

## Exporting configuration items from the source environment

---

You can export configuration items. The export process creates a JAR file, which is automatically saved to the repository. You can also download the migration file to save it locally.

### Before you begin

You must be logged in as an OpenPages administrator who has the **ExportConfiguration** application permission. You must also have read and write access to the **Migration Documents** folder. For more information, see “[Types of application permissions](#)” on page 52.

The export will fail if you have invalid triggers. Disable triggers before you export.

### About this task

#### Important:

- If a background import, export, or validate configuration process is currently running on the system, you must wait until processing is complete before submitting another configuration job.
- You cannot export while in System Admin Mode (SAM). For more information, see [Chapter 4, “System Admin Mode \(SAM\),” on page 37](#).
- The export will fail if you have invalid triggers. Disable triggers before you export.

### Procedure

1. Log on to the source OpenPages application as an administrator.
2. Disable System Admin Mode, if it is enabled. For more information, see “[Enabling and disabling System Admin Mode](#)” on page 37.
3. If you want to migrate hidden settings, set **Show Hidden Settings** to true.
4. Click  > **System Migration** > **Export Configuration**.
5. Click **Add Items**.
6. Select the items that you want to export.  
For example, if you want to export profiles, click **Object Profiles** and then select the profiles that you want to export.  
You can select items from multiple categories.
7. Click **Select**.
8. Review the list of selected items. If you want to change them, click **Edit Selections**.
9. Click **Save Migration File**.  
The **History** tab is displayed and the items are exported to a migration file in JAR format.  
The migration file is saved to the **Migration Documents** folder in the repository.
10. Optional: To download the migration file to your local system, click **Download**.

## Importing configuration items to the target environment

---

You can load the migration file into the target environment by downloading the file from the OpenPages repository or by importing a saved file from your local client.

The import process automatically validates the configuration items before performing the import to ensure that the items are complete and any object dependencies are in the migration file or in the target environment before the items are imported. The validation process verifies that:

- The XML file is a well-formed ObjectManager loader file.

- The metadata attributes are valid, according to the OpenPages validation rules.
- All dependent items that a particular item requires are present in either in the migration file or in the target system.
- Special characters are validated if the **Special Character Validation** setting is true (see “[Settings that apply to environment migration](#)” on page 719).

You can also run the validation process separately from the import. See “[Validating a migration file](#)” on page 728.

To avoid validation errors, review the information on dependent items that must be manually created and/or moved to the target environment. For details, see “[Items that are not migrated](#)” on page 722. For example, if you select a filter for import, ensure that all objects, field groups, and fields that are used by the filter are either included in the migration file or already in the target system.

You must have the **ImportConfiguration** application permission. You must also have read and write access to the **Migration Documents** folder. For information, see “[Types of application permissions](#)” on page 52 and “[Managing system files and folders](#)” on page 148.

**Important:** The environment migration import process might periodically enable System Admin Mode (SAM), preventing users from making and saving changes (see “[Enabling and disabling System Admin Mode](#)” on page 37). To avoid errors in the imported data and other issues, migrate data during off-hours or when the target environment is not being used.

## Configuring environment migration to allow special characters

The environment migration import process checks for any special characters in the name of the items being imported. By default, if any item has a name with a special character, the import stops. To import metadata items that use special characters in their names, you must disable this validation.

### Procedure

1. Access the **Settings** page (see Chapter 20, “[Viewing the Configuration and Settings page](#),” on page 473).
2. Go to the **Applications > GRCM > Environment Migration > Special Character Validation** setting.
3. In the **Value** box, type one of the following values:

*Table 222. Special Character Validation setting*

If the value is set to...	Then...
true	The import process checks for special characters in the name of metadata items being imported. This value is the default.
false	The import process allows metadata items with special characters in the name to be imported.

4. Click **Done**.

## Validating a migration file

This task is optional. The import process validates migration files automatically, but you can also run a validation separately from an import.

**Important:** If a background import, export, or validate configuration process is currently running on the system, you must wait until processing is complete before submitting another configuration job.

If you are importing an XML format file, you must use the following file naming convention:

```
<loader-file-prefix>-op-config.xml
```

## Procedure

1. Log on to the target OpenPages application as a user with the **Import Configuration** permission.
2. Click  > **System Migration** > **Import Configuration**.
3. Select the migration file.
  - If the migration file is on your local system, click **Local drive**, and then click **Add file**.
  - If the migration file is in the repository, click **Server repository**, and then click the file that you want to validate.
4. Click **Validate**.

## Results

If **The requested operation could not be completed** is displayed, check the migration file. The file must be either a migration JAR file or an ObjectManager XML file.

If **Completed With Errors** is displayed, review the status messages on the **History** tab for information about the errors. You must fix validation errors before you import the migration file.

## Importing a migration file

Use the following instructions to import configuration changes by using **Import Configuration**.

**Important:** Do not manually make changes to the application configuration during the import. Doing this can corrupt the data or result in errors. If this occurs, you must re-export the data before you attempt the import again.

### Before you begin

- If an import, export, or validate process is currently running on the system, you must wait until processing is complete before you submit another import, export, or validate job.
- The source and target environments must have the same version and patch level of OpenPages.
- Ensure that any dependencies that are not included the migration file are imported first. For example, if you are migrating profiles and the profiles use embedded reports on the home page, import the reports manually before you import the profiles.

## Procedure

1. Log on to the target OpenPages application as a user with the **ImportConfiguration** permission and read and write to the **Migration Documents** folder.
2. Click  > **System Migration** > **Import Configuration**.
3. Select the migration file (.jar or .xml).
  - If the migration file is on your local system, click **Local drive**, and then click **Add file**.
  - If the migration file is in the repository, click **Server repository**, and then click the file that you want to import.
4. Click **Import**.

The **Review Items** pane shows the items that will be imported, if those items are supported by the environment migration user interface. If you are importing other items, such as role templates, the items are not displayed, but they are imported. For more information, see [“Supported migration items” on page 720](#).

## Results

If **The requested operation could not be completed** is displayed, check the migration file. The file must be either a migration JAR file or an ObjectManager XML file.

If Completed With Errors is displayed, review the status messages on the **History** tab for information about the errors and review the “Environment migration best practices” on page 725. You must fix the errors before you import the migration file.

# Chapter 27. The ObjectManager tool

The ObjectManager tool provides a command-line interface (CLI) that you can use instead of the application graphical user interface to load data into the IBM OpenPages with Watson repository.

With the ObjectManager tool, you can perform the following tasks:

- Import (load) data, such as objects and configuration data, into the OpenPages with Watson repository.
- Export (dump) filtered or unfiltered data from the OpenPages with Watson repository. You can use this functionality, for example, to migrate environments and data from one computer to another one in a multi-deployment environment.
- Batch-load multiple loader files in a single session.

Only a Super Administrator has full access to ObjectManager operations.

If you use ObjectManager to load data from one environment into another, the source and target environments must have the same version and patch level of OpenPages with Watson.

For an alternative to using the ObjectManager tool, use  > **System Migration** > **Import Configuration**. You can use it to load system data, user-related information, and instance data. The rules that apply to loader files that are imported with the ObjectManager tool apply also to **Import Configuration**.

You can change the ObjectManager configuration settings, such as the maximum size of requests that are sent from ObjectManager to the REST API. For more information, see “[Tools properties and parameters](#)” on page 934.

## Working with loader files

The ObjectManager tool uses XML loader files to load (import) or dump (export or extract) data into IBM OpenPages with Watson.

The loader file name consists of a prefix, which is defined by the user, and a standard string that has the following format:

```
<loader-file-prefix>-op-config.xml
```

Where:

- <loader-file-prefix> is the user-defined portion of the loader file name.
- -op-config.xml is the standard string that follows the prefix and identifies the file as a loader file to the ObjectManager tool. Do not change this portion of the file name.

When you pass a loader file parameter to the ObjectManager tool, you pass only the prefix portion of the loader file name. If no prefix is provided, the ObjectManager tool attempts to load from or write to the file op-config.xml.

**Note:** If you use ObjectManager to import security rules, any existing security rules are overwritten by the import.

### Import example

If you want to load (import) data into the OpenPages with Watson repository, you could, for example, create a loader file with the name mydata-op-config.xml (prefix + standard string). When you pass the prefix mydata to the ObjectManager tool, the ObjectManager tool automatically looks for a loader file that is named mydata-op-config.xml.

## Export example

If you want to extract (dump) data from OpenPages with Watson, you could, for example, pass the prefix myconfig to the ObjectManager tool. The ObjectManager tool automatically creates an export (dump) file that is named myconfig-op-config.xml.

## Creating a data loader file

A data loader file is an XML file that contains the data you want to import or load through the ObjectManager into your system.

You can use any XML or text editor of your choice to create a data loader file.

After you create the data loader file, save it using the file naming convention described in [“Working with loader files” on page 731](#).

All element tags in a data loader file are nested within the root element <openpagesConfiguration xmlFormatVersion="1.31"> and </openpagesConfiguration> tags.

An ObjectManager data loader file has the following structure:

```
<?xml version="1.0" encoding="UTF-8"?>
<openpagesConfiguration xmlFormatVersion="1.31">
 <parent-element>
 <child-element/>
 <child-element/>
 </parent-element>
</openpagesConfiguration>
```

Where:

parent-element is a tag identifying the type of information to be loaded.

child-element is a nested tag within a given information type that usually contains attributes and/or text content.

The following code example shows the structure of an XML data loader file that, when loaded through the ObjectManager tool, updates the currency exchange rates for the Canadian dollar (CAD) and Mexican peso (MXN).

The exchangeRates element contains the exchangeRate child-element, which has attributes for the 3-letter ISO code for the country or region and the updated exchange rate for that currency. The rate can use up to eight decimal places.

```
<?xml version="1.0" encoding="UTF-8"?>
<openpagesConfiguration xmlFormatVersion="1.31">
 <exchangeRates>
 <exchangeRate isoCode="CAD"
 startDate="2020-05-09 17:36:12"
 rate="0.8636" />
 <exchangeRate isoCode="MXN"
 startDate="2020-05-09 17:36:12"
 rate="0.0951" />
 </exchangeRates>
</openpagesConfiguration>
```

## Running ObjectManager commands

The ObjectManager command file is named ObjectManager.cmd on computers running a Microsoft Windows operating system. The command file is named ObjectManager.sh on computers running a Linux operating system.

The file is located in the <OP\_HOME>/bin directory on OpenPages with Watson application servers.

*Table 223. Installation location of the OpenPages with Watson application*

<b>Operating system</b>	<b>Installation location</b>
Windows	For example, <OP_HOME> C:\IBM\OpenPages
Linux	For example, <OP_HOME> /opt/IBM/OpenPages

**Tip:** You can also run ObjectManager from a remote system, such as your laptop. For more information, see [“Installing tools and utilities \(IBM OpenPages with Watson\)” on page 692](#).

The ObjectManager command line must be:

- Run from the bin folder.
- Typed on a single line (no line breaks) in a command window.

**Important:** When using the ObjectManager tool, make sure that the OpenPages with Watson application services are running.

## Interactive command line loader file syntax

The ObjectManager tool uses the following syntax for a loader file.

**Note:** Make sure to run the command on a single line in the Command Prompt window.

```
ObjectManager <command> config|c <user> <password> <loader-file-path> <loader-file-prefix>
```

## ObjectManager command line parameters

You can use various commands and parameters with the ObjectManager tool.

### <command>

Required.

Value can be one of the following:

- dump or d - dumps or exports data.
- load or l - loads or imports data from a single loader file.
- validate or v - certifies or compares data.

### <batch-mode>

Places ObjectManager in batch processing mode. Loads multiple loader files in a single session.

Value is batch or b.

For more information, see [“Batch loader file syntax and sample” on page 735](#).

### <user> and <password>

Required.

Some actions may require a Super Administrator account.

Both parameters are used for authentication. You can use your user ID and your password.

When you are running ObjectManager on IBM Cloud Pak for Data, use one of the following combinations instead of your user ID and password:

- jwt and a IBM Cloud Pak for Data JSON Web Token (JWT)
- Your IBM Cloud Pak for Data user name and your IBM Cloud Pak for Data API key

An API Key can be generated in IBM Cloud Pak for Data. For more information, see [Generating API keys for authentication](#).

To see examples of using these parameters in IBM OpenPages for IBM Cloud Pak for Data, see [“Load command example” on page 734](#).

**<loader-file-path>**

Optional.

The file path to a single XML loader file.

By default, this is the current directory if no file path is specified.

The ObjectManager.log file is written to this directory.

**<batch-loader-dir>**

Optional.

The directory path to the XML loader files that are listed in the <batch-loader-list-file>. Can be a top-level directory if loader files are in multiple sub-folders under that directory.

**<loader-file-prefix>**

Optional.

The user-defined portion of the loader file name.

By default, the ObjectManager tool attempts to load from or write to the file op-config.xml, if no prefix is specified.

**<batch-loader-list-file>**

Required.

The fully qualified file path and name of a text document containing a list of loader files for batch processing.

## Load command example

This Windows-based example shows how to use a loader file that is named data1-op-config.xml that resides in the c:\import folder to load or import data into IBM OpenPages with Watson.

This example uses the Super Administrator account, OpenPagesAdministrator.

### Procedure

1. Open a Command Prompt window.
2. Navigate to the bin directory, for example:

```
cd C:\OpenPages\bin
```

3. Run the following command on a single line to load the data1-op-config.xml loader file:

```
ObjectManager l c OpenPagesAdministrator <password> c:\import data1
```

The log file is c:\import\ObjectManager.log.

If you are running ObjectManager on Cloud Pak for Data, use one of the following options to specify the user name and password in a command:

- Use jwt and a Cloud Pak for Data JSON Web Token (JWT) as in the following example:

```
ObjectManager l c jwt <JSON-Web-Token> c:\import data1
```

- Use your Cloud Pak for Data user name and your Cloud Pak for Data API key as in the following example:

```
ObjectManager l c admin <API-Key> c:\import data1
```

An API Key can be generated in Cloud Pak for Data. For more information, see [Generating API keys for authentication](#).

## Dump command example

This Windows-based example shows how to export or dump data from IBM OpenPages with Watson to a file with the config1 prefix that resides in the c :\export folder. If the folder does not already exist, the ObjectManager tool creates it. This example uses the Super Administrator account, OpenPagesAdministrator.

### Procedure

1. Open a Command Prompt window.
2. Navigate to the bin directory, for example:

```
cd C:\OpenPages\bin
```

3. Run the following command on a single line to export data from OpenPages with Watson into the config1-op-config.xml loader file:

```
ObjectManager d c OpenPagesAdministrator OpenPagesAdministrator c:\export config1
```

The file named config1-op-config.xml is created in the c :\export folder.

## Batch loader file syntax and sample

A batch loader list file is typically a text (.txt) file that contains a list of the XML loader files for batch processing by the ObjectManager tool.

The ObjectManager tool uses the following syntax for batch loading multiple loader files.

```
ObjectManager <batch-mode> config|c <user> <password> <batch-loader-dir> <batch-loader-list-file>
```

A batch loader list file uses the following rules:

- Any line starting with a number sign (#) is considered a comment
- Any line starting with greater than sign (>) is written to the screen for display
- All other lines are assumed to be the relative path to a loader file

The following sample batch loader list file was created in a text editor. It shows how to display an informational "loading" message (line starting with >) on the screen for files that are loading from different directories, and provides an example of how to list a loader file (example1-op-config.xml) from a top-level (c :\temp) directory and how to list multiple loader files (example2, example3, example4) from a subfolder (\loaders) located under the top-level directory.

```
If the <batch-loader-dir> was given as c:\temp, the following lines would
write the "Loading..." message and then attempt to load the file
c:\temp\example1-op-config.xml
>Loading example 1...
example1

If the <batch-loader-dir> was given as c:\temp, the following lines would
write the "Loading..." message and then attempt to load the files:
c:\temp\loaders\example2-op-config.xml
c:\temp\loaders\example3-op-config.xml
c:\temp\loaders\example4-op-config.xml
>Loading examples 2-4...
loaders\example2
loaders\example3
loaders\example4
```

For example, you save this batch loader list file with the name load-reports.txt in the c :\OpenPages default installation directory.

The instructions in the following example show how to run the sample `load-reports.txt` batch loader list file to load or import data into IBM OpenPages with Watson. The top-level directory (`c:\temp`) is used for the `<batch-loader-dir>` parameter because it includes the loader files in the `\loaders` subfolder.

## Procedure

1. Open a Command Prompt window.
2. Navigate to the `bin` directory, for example:

```
cd C:\OpenPages\bin
```

3. Run the following batch command to load the `load-reports.txt` batch loader list file:

```
ObjectManager b c OpenPagesAdministrator password c:\temp load-reports.txt
```

## Using ObjectManager to move objects

This example shows how an IBM OpenPages with Watson administrator can move a process object from the folder location `/ENTITY02` to `/ENTITY01`.

### Before you begin

This solution assumes that the administrator knows the following:

- The contents of TechNote # 1648075 that explains the difference between system folder location and associations.
- The system-level folder name of the object.
- The target folder location already exists. Otherwise, the following validation will occur:

```
VALIDATION ERROR (Line: 967 Column: 89): Target Folder Resource
(/_op_sox/Project/Default/ICDocumentation/Processes/SampleFolder001)
does not exist.
```

### About this task

The following is the syntax for moving objects using the ObjectManager tool:

```
<openpagesConfiguration xmlFormatVersion="1.31">
 <moveResources>
 <targetFolder name="{fullpath of target folder}">
 <sourceResource name="{fullpath of the object to be moved}" />
 </targetFolder>
 </moveResources>
</openpagesConfiguration>
```

## Procedure

1. Log on to the application server.
2. Open a text editor.
3. Copy the previous syntax example.
4. Update the example to reflect the target folder location(s) and source folder location(s).

For example:

```
<openpagesConfiguration xmlFormatVersion="1.31">
 <moveResources>
 <targetFolder name="/_op_sox/Project/Default/ICDocumentation/
 Processes/ENTITY01">
 <sourceResource name="/_op_sox/Project/Default/ICDocumentation/
 Processes/ENTITY02/PROC01.txt"/>
 </targetFolder>
 </moveResources>
</openpagesConfiguration>
```

5. Save the file using the an ObjectManager name (e.g., `samplemove-op-config.xml`).

6. Open a command prompt or shell. Alternatively, you can use  > **System Migration** > **Import Configuration** to import the XML file. For information, see “[Importing a migration file](#)” on page 729.
7. Go to *OP\_HOME/bin* where *OP\_HOME* represents the installation location of the OpenPages with Watson application.
8. Run the command to load the ObjectManager file.

The following is the sample output for the working example:

```
D:\OpenPages\bin>ObjectManager l c
OpenPagesAdministrator OpenPagesAdministrator
D:\temp samplemove

OpenPages V8.1.0.0 (Build: OP_8.1-270 2019/09/06 19:17:21) starting ...
OpenPages Global environment initialized.
=====
Object Manager Admin Utility V8.1.0.0 (Build: OP_8.1-270 2019/09/06 19:27:49)
=====

List of command line arguments:
 Arg 1: <l>
 Arg 2: <c>
 Arg 3: <OpenPagesAdministrator>
 Arg 4: <*****>
 Arg 5: <D:\temp>
 Arg 6: <samplemove>
Total number of arguments: 6
OpenPages Server environment initialized.

Loading OpenPages Configuration (samplemove) from folder: 'D:\temp' ...

Processing started at Thu Apr 05 15:51:29 EDT 2013

Processing Move Resource Requests ...
 1 total

Move Resource requests processed: 1

Total Objects processed: 0

Total Requests processed: 1

Total Validation Errors: 0

Total Exceptions: 0

Processing finished at Thu Oct 03 15:51:29 EDT 2019
Elapsed time: 347 milliseconds
```

9. Restart the OpenPages services. For more information, see [Chapter 25, “Starting and stopping servers,” on page 709](#).
10. If an administrator needs to move multiple objects via ObjectManager, the following is the sample syntax:

```
<openpagesConfiguration xmlFormatVersion="1.31">
 <moveResources>
 <targetFolder name="{target fullpath folder for object 1}">
 <sourceResource name="{fullpath of the object 1 to be moved}" />
 </targetFolder>
 <targetFolder name="{target fullpath folder for object 2}">
 <sourceResource name="{fullpath of the object 2 to be moved}" />
 </targetFolder>
 <targetFolder name="{target fullpath folder for object 3}">
 <sourceResource name="{fullpath of the object 3 to be moved}" />
 </targetFolder>
 </moveResources>
</openpagesConfiguration>
```

## Using ObjectManager to rename objects

This example shows how an IBM OpenPages with Watson administrator can rename an entity from ENTITY01 to ENTITY01A.

## Before you begin

The following solution assumes that the administrator knows the system-level folder name of the object. Otherwise, the following message will be displayed:

```
VALIDATION ERROR (Line: 968 Column: 55): Resource to rename
(/_op_sox/Project/Default/BusinessEntity/ENTITY_oldname/ENTITY_oldname.txt)
does not exist.
```

## About this task

The following is the ObjectManager syntax for renaming objects:

```
<openpagesConfiguration xmlFormatVersion="1.31">
 <renameResources>
 <renameResource oldFullName="{fullpath of the object to be renamed}"
 newShortName="{name new of the object}.txt"/>
 </renameResources>
</openpagesConfiguration>
```

## Procedure

1. Log on to the application server.
2. Open a text editor.
3. Copy the previous syntax example.
4. Update the example to reflect the target folder location(s) and source folder location(s).

For example:

```
<openpagesConfiguration xmlFormatVersion="1.31">
 <renameResources>
 <renameResource oldFullName="/_op_sox/Project/Default/
 BusinessEntity/ENTITY01/ENTITY01.txt"
 newShortName="ENTITY01A.txt"/>
 </renameResources>
</openpagesConfiguration>
```

5. Save the file using the ObjectManager file name format, such as samplerename-op-config.xml.
6. Open a command prompt or shell. Alternatively, you can use  **System Migration > Import Configuration** to import the XML file. For information, see [“Importing a migration file” on page 729](#).
7. Go to *OP\_HOME/bin* where *OP\_HOME* represents the installation location of the OpenPages with Watson application.
8. Run the command to load the ObjectManager file.

The following is the sample output for the working example:

```
D:\OpenPages\bin>ObjectManager l c OpenPagesAdministrator
OpenPagesAdministrator D:\temp samplerename

OpenPages V8.1.0.0 (Build: OP_8.1-270 2019/09/06 19:17:21) starting ...
OpenPages Global environment initialized.
=====
Object Manager Admin Utility V8.1.0.0 (Build: OP_8.1-270 2019/09/06 19:27:49)
=====

List of command line arguments:
 Arg 1: <l>
 Arg 2: <c>
 Arg 3: <OpenPagesAdministrator>
 Arg 4: <*****>
 Arg 5: <D:\temp>
 Arg 6: <samplerename>
Total number of arguments: 6
OpenPages Server environment initialized.

Loading OpenPages Configuration (samplerename) from folder: 'D:\temp' ...
Processing started at Fri Apr 05 08:48:21 EDT 2013
Processing Rename Resource Requests ...
 1 total
```

```

Rename Resource requests processed: 1
Total Objects processed: 0
Total Requests processed: 1
Total Validation Errors: 0
Total Exceptions: 0
Processing finished at Fri Oct 04 08:48:23 EDT 2019
Elapsed time: 2418 milliseconds

```

9. Restart the OpenPages services. For more information, see [Chapter 25, “Starting and stopping servers,” on page 709](#).

If an administrator needs to rename multiple objects via ObjectManager, the following is the sample syntax:

```

<openpagesConfiguration xmlFormatVersion="1.31">
 <renameResources>
 <renameResource oldFullName="{fullpath of the object 1 to be renamed}"
 newShortName="{name new of the object 1}.txt"/>
 <renameResource oldFullName="{fullpath of the object 2 to be renamed}"
 newShortName="{name new of the object 2}.txt"/>
 <renameResource oldFullName="{fullpath of the object 3 to be renamed}"
 newShortName="{name new of the object 3}.txt"/>
 </renameResources>
</openpagesConfiguration>

```

## Using ObjectManager to assign or revoke role assignments

An IBM OpenPages with Watson administrator can assign or revoke role assignments using the ObjectManager tool.

### Before you begin

This solution assumes that the administrator knows the following items:

- The system-level folder name of the security domain.
- The role assignment type of the role template.
- The role template name.
- The OpenPages with Watson user name.

### About this task

The ObjectManager syntax for revoking or assigning a role assignment is as follows:

```

<?xml version="1.0" encoding="UTF-8"?>
<openpagesConfiguration xmlFormatVersion="1.31">
 <roleAssignments>
 <roleAssignment type="{object type}" status="{assign/revoke}">
 <businessUnits>
 <businessUnit name="{path of the security domain}" />
 </businessUnits>
 <roleActors>
 <roleActor name="{actorname}" />
 </roleActors>
 <roles>
 <role name="{role template name}" />
 </roles>
 </roleAssignment>
 </roleAssignments>
</openpagesConfiguration>

```

Using the following example, an administrator can revoke the user `johndoe` from the root level security domain.

## Procedure

1. Log on to the application server.
2. Open a text editor.
3. Copy the syntax example.
4. Update the example to reflect the correct role assignment type: whether to assign or revoke the role; the security domain path; name of actor; and the role template name. For example:

```
<?xml version="1.0" encoding="UTF-8"?>
<openpagesConfiguration xmlFormatVersion="1.31">
 <roleAssignments>
 <roleAssignment type="SOXBusEntity" status="revoke">
 <businessUnits>
 <businessUnit name="/" />
 </businessUnits>
 <roleActors>
 <roleActor name="johndoe"/>
 </roleActors>
 <roles>
 <role name="OpenPages Modules 7.0 - All Data - No Admin"/>
 </roles>
 </roleAssignment>
 </roleAssignments>
</openpagesConfiguration>
```

5. Save the file using the ObjectManager file name format, such as groupmem-revoke-op-config.xml.
6. Open a command prompt or shell. Alternatively, you can use  > **System Migration > Import Configuration** to import the XML file. For information, see [“Importing a migration file” on page 729](#).
7. Go to *OP\_HOME\bin* folder.
8. Run the command to load the ObjectManager file.

The following extract is the sample output for the working example:

```
OpenPages V8.1.0.0 (Build: OP_8.1-270 2019/09/06 14:20:23)
starting ...
OpenPages Global environment initialized.
=====
Object Manager Admin Utility V8.1.0.0
(Build: OP_8.1.0.0-270 2019/09/06 14:20:23)
=====

List of command line arguments:
Arg 1: <load>
Arg 2: <config>
Arg 3: <OpenPagesAdministrator>
Arg 4: <*****>
Arg 5: <C:\temp>
Arg 6: <groupmem-revoke>
Total number of arguments: 6
OpenPages Server environment initialized.

Loading OpenPages Configuration (groupmem-revoke) from folder:
'C:\temp' ...

Processing started at Fri Jun 13 14:00:52 EDT 2014

Loading Role Assignments ...
 1 total

Role Assignments processed: 1
Business Units processed: 1
Role Actors processed: 1
Roles processed: 1

Total Objects processed: 4
Total Validation Errors: 0

Total Exceptions: 0
Processing finished at Fri Jun 13 14:00:58 EDT 2014
Elapsed time: 5703 milliseconds
```

9. Restart the OpenPages services. For more information, see [Chapter 25, “Starting and stopping servers,” on page 709](#).

## Using ObjectManager to create or load users

This example shows how an IBM OpenPages with Watson administrator can create or load users into the system.

### Before you begin

This solution assumes that the OpenPages administrator has already created the groups that are referenced in the example.

### About this task

The following is the syntax for creating or loading users by using the ObjectManager tool:

```
<openpagesConfiguration xmlFormatVersion="1.31">
 <actors>
 <actor>
 name="{username}"
 type="User"
 password="{password}"
 firstName="{firstname}"
 middleName=""
 lastName="{lastname}"
 canChangePassword="{true/false}"
 isTemporaryPassword="{true/false}"
 passwordExpiresInDays="0"
 description=""
 emailAddress="{email_address}"
 locale="{locale}"
 adminLevel="Default"
 enabled="true"
 hidden="false"
 editable="true"
 </actor>
 </actors>
 <actorGroupMemberships>
 <actorGroupMembership name="{username}" isEntityGroup="false">
 <group name="{existing_group_name}" isEntityGroup="false"/>
 <group name="OpenPages" isEntityGroup="false"/>
 </actorGroupMembership>
 </actorGroupMemberships>
</openpagesConfiguration>
```

### Procedure

1. Log on to the application server.
2. Open a text editor.
3. Copy the syntax example that is included earlier in this topic into the text editor.
4. Modify the example to reflect the actual users and groups details. For example, you can modify the example in the following way:

```
<openpagesConfiguration xmlFormatVersion="1.31">
 <actors>
 <actor>
 name="johndoe"
 type="User"
 password="openpages123"
 firstName="John"
 middleName=""
 lastName="Doe"
 canChangePassword="true"
 isTemporaryPassword="false"
 passwordExpiresInDays="0"
 description=""
 emailAddress="john.doe.user@company.com"
 locale="U.S. English"
 adminLevel="Default"
```

```

 enabled="true"
 hidden="false"
 editable="true">
 </actor>
</actors>
<actorGroupMemberships>
 <actorGroupMembership name="johndoe" isEntityGroup="false">
 <group name="All_Users" isEntityGroup="false"/>
 <group name="OpenPages" isEntityGroup="false"/>
 </actorGroupMembership>
</actorGroupMemberships>
</openpagesConfiguration>

```

5. Save the file using the ObjectManager file name format, such as `loadusers-op-config.xml`.
6. Open a command prompt or a shell and follow the instructions below. Alternatively, you can use  > **System Migration > Import Configuration** to import the XML file. For information, see “[Importing a migration file](#)” on page 729.
7. Go to `OP_HOME/bin` directory where `OP_HOME` represents the installation location of the OpenPages with Watson application.
8. Run the command to load the ObjectManager file. The following is the sample output for the example:

```

=====
ObjectManager Admin Utility V8.1.0.0
=====
List of command line arguments:
Arg 1: <l>
Arg 2: <c>
Arg 3: <OpenPagesAdministrator>
Arg 4: <****>
Arg 5: <C:\temp>
Arg 6: <loadusers>
Total number of arguments: 6
OpenPages Server environment initialized.

Loading OpenPages Configuration (userz2) from folder: 'C:\temp' ...
Processing started at Mon Oct 23 14:00:00 EST 2019

Loading Actors ...
1 total

Loading Actor Group Memberships ...
1 total

Actors processed: 1 (1 updated)
Actor Group Memberships processed: 1

Total Objects processed: 2

Total Validation Errors: 0

Total Exceptions: 0

Processing finished at Mon Feb 23 14:00:59 EST 2015
Elapsed time: 454 milliseconds

C:\OpenPages\bin>

```

9. Restart the OpenPages services. For more information, see [Chapter 25, “Starting and stopping servers,” on page 709](#).

## Modifying the ObjectManager properties file

The `ObjectManager.properties` file contains settings that control or limit the scope of exported (dumped) configuration and related data from the ObjectManager tool.

Depending on your export activity, modify the value of configuration or migration settings. Edit the `ObjectManager.properties` file in any text editor.

**Note:** Before you modify the `ObjectManager.properties` file, make a backup copy of the file.

For a list of settings and descriptions, see “[Settings in the ObjectManager.properties file](#)” on page 743.

To determine whether the settings in the file require modification, refer to the following topics:

- “[Exporting all currency exchange rates](#)” on page 753
- “[Exporting currency field definitions](#)” on page 755
- “[Exporting computed field definitions](#)” on page 756
- “[Exporting file attachments](#)” on page 756
- “[Migrating configuration changes using the ObjectManager tool](#)” on page 760

The `ObjectManager.properties` file is located in the `<OP_HOME>/bin` directory of your IBM OpenPages with Watson installation.

Table 224. Installation location of the OpenPages with Watson application	
Operating system	Installation location
Windows	For example, <code>&lt;OP_HOME&gt; C:\IBM\OpenPages</code>
Linux	For example, <code>&lt;OP_HOME&gt; /opt/IBM/OpenPages</code>

## Settings in the `ObjectManager.properties` file

The `ObjectManager.properties` file contains several settings or properties that you can configure.

### The logger property

#### `object.manager.logger.settings`

Defines the location of the logging properties file relative to the bin directory. Do not change this setting.

```
object.manager.logger.settings=../log4j2.properties
```

### The `configuration.manager.migrate.configuration.objects`

The `configuration.manager.migrate.configuration.objects` property overwrites the following `configuration.manager.dump.*` properties and is the equivalent of setting these properties to true:

- `configuration.manager.dump.bundle.types`
- `configuration.manager.dump.file.upload.content.types`
- `configuration.manager.dump.jsp_based.content.types`
- `configuration.manager.dump.admin.objectprofile.views`
- `configuration.manager.dump.form_based.content.types`
- `configuration.manager.dump.object.profiles`
- `configuration.manager.dump.application.string.key.categories`
- `configuration.manager.dump.application.string.keys`
- `configuration.manager.dump.application.strings`
- `configuration.manager.dump.object.strings`
- `configuration.manager.dump.error.strings`
- `configuration.manager.dump.querydefinitions`
- `configuration.manager.dump.field.dependency`
- `configuration.manager.dump.field.dependency.picklist`
- `configuration.manager.dump.recursive.hierarchy`
- `configuration.manager.dump.date.dimension.type`

- configuration.manager.dump.object.type.dimension
- configuration.manager.dump.date.dimension.type.associations
- configuration.manager.dump.recursive.hierarchy.strings
- configuration.manager.dump.date.dimension.type.strings
- configuration.manager.dump.object.type.dimension.strings
- configuration.manager.dump.content.type.relationship.sets
- configuration.manager.dump.actor.object.profile.associations
- configuration.manager.dump.locales
- configuration.manager.dump.role.templates
- configuration.manager.dump.role.administrators
- configuration.manager.dump.role.assignments
- configuration.manager.dump.subsystem.exclusion.fields
- configuration.manager.dump.registry
- configuration.manager.dump.processdefinitions
- configuration.manager.dump.tbrules
- configuration.manager.dump.tbcalculations

Additionally, the `configuration.manager.migrate.configuration.objects` property exports the following data:

- Any object folders referenced by:
  - jsp.based.content.types
  - form.based.content.types
- query definition (filter) strings
- reporting schema column definitions (which are used to keep framework labels consistent when you have duplicate field names).

## The `configuration.manager.dump.*` export properties

The following list describes the behavior of the various export `configuration.manager.dump.*` properties when a property is enabled (the value is set to `true`).

### `configuration.manager.dump.modules`

Exports a list of the modules (solutions) that are installed. It also controls the list of entries on the **About OpenPages with Watson** and **Build Information** pages.

### `configuration.manager.dump.file.types`

Exports a list of valid file attachment types (such as docx, pdf, jpg).

### `configuration.manager.dump.bundle.types`

Exports all field groups in the system, along with all of their fields.

### `configuration.manager.dump.file.upload.content.types`

Exports all file upload object types, such as **SOXDocument**. It will also export any folders (`nonFormBasedResources`) that are referenced by these object types.

### `configuration.manager.dump.jsp.based.content.types`

Exports all other object types, such as **SOXBusEntity**, **Mandate**, and **Policy**. It will also export any folders (`nonFormBasedResources`) that are referenced by these object types.

### `configuration.manager.dump.content.type.relationship.sets`

Exports a list of which objects types can be associated to what other object types.

### `configuration.manager.dump.app.permissions`

Exports a list of application permissions that can be granted to groups or role templates.

**configuration.manager.dump.actors**

Exports all users, groups, and security domain groups.

**configuration.manager.dump.actor.group.memberships**

Exports all group memberships, such as: which users belong to what groups, which users belong to what security domains, and which security domains belong to what other security domains.

**configuration.manager.dump.actor.object.profile.associations**

Exports users and groups and their assigned profiles.

**configuration.manager.dump.admin.objectprofile.views**

Exports object profiles. This property should be used with the configuration.manager.dump.object.profiles setting.

**configuration.manager.dump.objectprofiles**

Exports object profiles. This property should be used with the configuration.manager.dump.admin.objectprofile.views setting.

**configuration.manager.dump.non.form.based.resources**

Exports all folders and object instances in the system. You can use the setting configuration.manager.dump.resources.root.folder to narrow the scope of objects that are exported. You will probably want to use this setting with the setting configuration.manager.dump.resource.sets.

As an alternative, you can use the configuration.manager.dump.associated.resources property.

**configuration.manager.dump.form.based.content.types**

Exports form-based object type definitions if these were used. By default (out of the box), the software does not use form-based object type definitions.

**configuration.manager.dump.form.based.resources**

Exports instances of form-based object types if these were used. This property is similar to the configuration.manager.dump.non.form.based.content.types property.

The configuration.manager.dump.form.based.resources property is generally not needed because of what is stated in the configuration.manager.dump.form.based.content.types property.

**configuration.manager.dump.channels**

Exports all reports that appear on the **Reporting** menu in the IBM OpenPages with Watson application, such as: all JSP reports and any Cognos reports that have been published to the OpenPages with Watson application. It does not export any report definitions from Cognos. If you want to export JSP report definitions, you will also want to set the configuration.manager.dump.non.form.based.resources property to true, and the configuration.manager.dump.resources.root.folder property to /Reports.

**configuration.manager.dump.resource.sets**

Exports object instance relationships. For example, if you had an entity called Entity ABC that had a child process called Process A, you would set the following properties to true:

- configuration.manager.dump.non.form.based.resources property to get the definitions of Entity ABC and Process A
- configuration.manager.dump.resource.sets property to get the entry that says Process A is a child of Entity ABC.

As an alternative, you can use the configuration.manager.dump.associated.resources property.

**configuration.manager.dump.associated.resources**

Exports objects and their relationships – you can use it instead of configuration.manager.dump.non.form.based.resources and configuration.manager.dump.resource.sets.

To filter the scope of the export, you can use the following settings:

**configuration.manager.dump.associated.resources.set**

The value of this setting, SOX.ProjectDefault, is a constant, do not change it.

**configuration.manager.dump.associated.resources.label**

Enter the name of the reporting period from which you want to export data. If you leave this value blank, it will default to the **Current Report Period**.

**configuration.manager.dump.associated.resources.root.node.****[number]**

You can create multiple entries with this setting if you increment the *[number]* part of the name. Enter the full paths of the objects (one object per entry) that you want to use as the scope for the data export. To find the full path of the object, you may need to look at the object in OpenPages. The default value of /\_op\_sox/Project/Default/Default.txt will export all of the data in the system.

**configuration.manager.dump.associated.resources.include.content.type.****[number]**

You can create multiple entries with this setting if you increment the *[number]* part of the name.

Enter one object type name per entry that you want to include in the export. As the export process navigates the object tree structure in the system, when it encounters an object that is not of a type listed in these entries, it will not export that object or any of its children. In this way you can limit the scope of exported objects. A blank entry value will include all object types.

To filter export results, add entry values to one of the following settings. Adding entry values to both settings is redundant.

```
configuration.manager.dump.associated.resources.include.content.type.
[number]
```

```
configuration.manager.dump.associated.resources.exclude.content.type.
[number]
```

**configuration.manager.dump.associated.resources.exclude.content.type.****[number]**

You can create multiple entries with this setting if you increment the *[number]* part of the name. Enter one object type name per entry that you want to exclude in the export. As the export process navigates the object tree structure in the system, when it encounters an object that is not of a type listed in these entries, it will not export that object or any of its children. In this way you can limit the scope of exported objects. A blank entry value will include all object types.

**configuration.manager.dump.rule.sets**

Exports all object reset rule sets.

**configuration.manager.dump.rule.set.execute.sessions**

Exports the history of object reset executions.

**configuration.manager.dump.registry**

Exports all settings in the system.

To filter the scope of the export, you can use the following settings:

**configuration.manager.migrate.configuration.exclude.registry.entry.****[number]**

Excludes entries listed in this setting from export.

**configuration.manager.dump.registry.root.entry.****[number]**

Sets the scope of settings to be exported.

You can create multiple entries with this property by incrementing the *[number]* part of the name.

**configuration.manager.dump.recursive.hierarchy**

Exports recursive object levels.

**configuration.manager.dump.date.dimension.type**

Exports date dimension types.

- configuration.manager.dump.object.type.dimension**  
Exports object type dimensions.
- configuration.manager.dump.date.dimension.type.associations**  
Exports date dimension type associations (what date dimension types are enabled for what fields).
- configuration.manager.dump.locales**  
Exports supported locales (languages). No translations are included.
- configuration.manager.dump.application.string.key.categories**  
Exports the application text folders.
- configuration.manager.dump.application.string.keys**  
Exports application text keys – the list of entries on the **Application Text** page – without translations.
- configuration.manager.dump.application.strings**  
Exports translations for application text.
- configuration.manager.dump.recursive.hierarchy.strings**  
Exports translations for recursive object levels.
- configuration.manager.dump.date.dimension.type.strings**  
Exports translations for date dimension types.
- configuration.manager.dump.object.type.dimension.strings**  
Exports translations for object type dimensions.
- configuration.manager.dump.error.strings**  
Exports translations for error messages.
- configuration.manager.dump.object.strings**  
Exports translations for: object type names, field names, field guidance, section names, and enumerated values.
- configuration.manager.dump.job.types**  
Exports jobs from the Scheduler. It does not export workflows or Java classes that are used by the jobs.
- configuration.manager.dump.currency.exchange.rates**  
Exports exchange rates.
- configuration.manager.dump.currencies**  
Exports the list of valid currencies (enabled and disabled).
- configuration.manager.dump.querydefinitions**  
Exports public filters.
- configuration.manager.dump.user.preferences**  
Exports **Alert Notification** settings for each user.
- configuration.manager.dump.role.templates**  
Exports role templates.
- configuration.manager.dump.role.administrators**  
Exports which users are assigned as administrators for what security domains.
- configuration.manager.dump.role.assignments**  
Exports which users are assigned which role templates for what security domains.
- configuration.manager.dump.field.dependency**  
Exports field dependencies.
- configuration.manager.dump.field.dependency.picklist**  
Exports dependent picklists.
- configuration.manager.dump.subsystem.exclusion.fields**  
Exports fields that are excluded from the reporting subsystem.
- configuration.manager.dump.record.level.security.rulesets**  
Exports rule sets from record level security.
- configuration.manager.dump.processdefinitions**  
Exports GRC workflow definitions.

**configuration.manager.dump.dashboard.views**  
Exports dashboards.

**configuration.manager.dump.responsive.views**  
Exports views.

**configuration.manager.dump.tbrules**  
Exports rules from the **Rules Engine**.

**configuration.manager.dump.tbcalculations**  
Exports calculations from GRC Calculations.

**configuration.manager.dump.solutions**  
Exports solution visualizations.

**configuration.manager.dump.themes**  
Exports themes.

**configuration.manager.dump.tags**  
Exports tags.

## The configuration.manager.force.update.\* properties

**configuration.manager.force.update.object.strings**  
Overwrites existing object strings when set to true prior to a load.  
The default is false. If you change this setting to true, the load overwrites existing customized strings. Change it immediately back to false after the load is done to protect against inadvertently overwriting customized strings.

**configuration.manager.force.update.application.strings**  
Overwrites existing application strings when set to true prior to a load.  
The default is false. If you change this setting to true, the load overwrites existing customized strings. Change it immediately back to false after the load is done to protect against inadvertently overwriting customized strings.

## The invalid characters property

**configuration.manager.property.name.illegal.characters=!@#\$%^&\*()<>+=[]\/{|}?**  
Defines characters that cannot be used in field names.

## The disable triggers properties

**configuration.manager.migrate.configuration.disable.all.triggers=/OpenPages/Applications/GRCM/Disable Triggers**  
Points to the registry setting that indicates whether triggers are disabled or not. Do not change it. It works with the configuration.manager.disable.triggers setting.

**configuration.manager.disable.triggers**  
Disables triggers when importing or exporting data in order to not trigger excess processing as objects are created, modified, or associated. If set to true, triggers are disabled at the start of the import or export and re-enabled at the end. Default is false.

## The resource load property

**configuration.manager.load.resource.ignore.undefined.property.value**  
Controls behavior when loading objects. For more information, see “[Controlling data load behavior](#)” on page 751.

## Filtering data for export

---

By using a filters file with predefined filters, you can narrow the scope of configuration and related data that is exported from the IBM OpenPages with Watson repository by the ObjectManager tool.

## Before you begin

Before you can export selected data using a filters configuration file, you must verify that all dump configuration settings in the ObjectManager.properties file are correctly set.

Any settings in the ObjectManager.properties file that start with the following code must have its value set to true. If the value is set to false, then change the value to true.

```
configuration.manager.dump.<property>=true
```

For example, configuration.manager.dump.object.profiles=true

For details on modifying the ObjectManager.properties file, see [“Modifying the ObjectManager properties file” on page 742](#).

## About the filters configuration file

Filters are defined in an XML-based configuration file that must be named ObjectManagerExportFilters.xml. The file must be stored in the same directory as ObjectManager.cmd|sh, for example:

```
<OP_HOME>/bin/ObjectManagerExportFilters.xml
```

The XML tags used for specifying the predefined filters are the same as the ObjectManager configuration loader XML tags. Most filters are defined on the name attribute of an object. Some filters have either additional or different filter attributes.

For a list of predefined filters, see [Table 225 on page 749](#).

You can use the following sample file: <OP\_HOME>/bin/ObjectManagerExportFilters-Example.xml. Make a copy of the file, change the file name to ObjectManagerExportFilters.xml, make your changes, and copy the file to the directory where ObjectManager.cmd|sh is stored, for example <OP\_HOME>/bin.

### Example

The following sample filter code shows how you can use the ObjectManager tool to export only the object profile with the name Default. No other object types or any other profiles will be exported.

```
<objectProfiles>
 <!-- List of names of profiles to export -->
 <objectProfile name="Default"/>
</objectProfiles>
```

After defining the filters in the filters configuration file, you can use the ObjectManager dump command to export the objects.

## ObjectManager predefined filters

The following predefined filters are supported in the ObjectManager tool.

[Table 225 on page 749](#) lists the various element types with their corresponding element tag and filter attributes.

*Table 225. ObjectManager predefined filters*

Element type	Element tag	Filter attribute	Comment
Application Text	<application String>	name	The name of the application string.

Table 225. ObjectManager predefined filters (continued)

Element type	Element tag	Filter attribute	Comment
Channels	<channel>	Any of the following: <ul style="list-style-type: none"><li>• name</li><li>• channelFolder (name)</li><li>• pageTemplate (name)</li></ul>	The name of the reporting folder or path of the reporting folder or page template.
Currencies	<currency>	isoCode	The 3-letter ISO currency code.
Exchange Rates	<exchangeRate>	isoCode	The 3-letter ISO currency code.
Field Groups	<bundleType>	name	The name of the field group.
File based resources	<resource>	name	The full path of the resource.
Filters	<queryDefinition>	name	The name of the Query definition.
Job Types	<jobType>	name + (the associated bundles)	The name of the job type.
Object Profiles	<objectProfile>	name	The name of the object profile.
Object Profile Views	<objectProfileView>	Any of the following: <ul style="list-style-type: none"><li>• type</li><li>• name</li></ul>	Either the type only or the type and name of the Activity view.
Object Reset (SCOR) Rulesets	<ruleSet>	name	The name of the set.
Object Types	<contentType>	name	The name of the object type.
Object Type Pick List Dependencies	<dependencySet>	objectType	The object for which dependencies are defined.
Object Type Relationships	<contentType Relationship>	Any of the following: <ul style="list-style-type: none"><li>• parent</li><li>• child</li></ul>	The parent and/or child object types.
Object Text	Any of the following: <ul style="list-style-type: none"><li>• &lt;objectTypeString&gt;</li><li>• &lt;fieldString&gt;</li><li>• &lt;enumValueString&gt;</li><li>• &lt;viewString&gt;</li><li>• &lt;sectionString&gt;</li></ul>	name	The data for the selected string.

Table 225. ObjectManager predefined filters (continued)

Element type	Element tag	Filter attribute	Comment
Role Templates	<roleTemplate>	name	The name of the Role Template.
Settings	<registryEntry>	name	The name of the setting.
Sub-system Field Extensions	<subSystemExclusion ObjectType>	name	The name of the excluded object type.
User Group Memberships	<actorGroup Membership>	name	For all groups.
	<group>	name	For all group members.
Workflow definitions	<processDefinition>	<ul style="list-style-type: none"> <li>• name</li> <li>• objectType</li> </ul>	
Rules (in the <b>Rules Engine</b> )	<tbRule>	<ul style="list-style-type: none"> <li>• name</li> <li>• objectType</li> </ul>	

## Controlling data load behavior

To control the behavior of the ObjectManager tool when loading objects, you can modify a setting in the `ObjectManager.properties` file.

By setting the `configuration.manager.load.resource.ignore.undefined.property.value` in the `ObjectManager.properties` file, you can control whether the ObjectManager tool creates objects with undefined values (such as an empty value or a value without a default). This setting applies only to non-required fields.

**Note:** If a field is required and has no default value defined, then the ObjectManager tool:

- Ignores the setting in the `configuration.manager.load.resource.ignore.undefined.property.value` property
- Does not create the object instance
- Reports validation errors.

### Procedure

1. Open the `ObjectManager.properties` file in a text editor of your choice (see “[Modifying the ObjectManager properties file](#)” on page 742).
2. Set the value of the `configuration.manager.load.resource.ignore.undefined.property.value` property. If you set the value to:
  - `true` - then ObjectManager creates the object without validation errors. This value is the default.
  - `false` - then ObjectManager reports validation errors, does not create the object, and moves to the next object in the loader file.
3. Run the ObjectManager tool (see “[Running ObjectManager commands](#)” on page 732).

# Managing currency exchange rates

You can use XML elements in ObjectManager loader files to update, export, and enable or disable currency exchange rates.

**Note:** To use these functions, the currency must have a standard 3-letter ISO code and exist in your system.

There are several methods for updating currency exchange rates:

- Use the **Currencies** task. For more information, see [“Editing, enabling, disabling, and uploading currency exchange rates” on page 168](#).
- An ObjectManager loader file. For more information, see [“Importing exchange rates” on page 752](#).

## Importing exchange rates

Use a data loader file to import exchange rates for existing currency codes by specifying the new rates in the file or by uploading a properly formatted CSV file with the new rates.

**Note:** For CSV file format information, see [“Formatting a CSV file” on page 167](#).

### Before you begin

To use this function, the currency must have a standard three letter ISO code and exist in your system.

### Procedure

1. Create an XML data loader file (see [“Creating a data loader file” on page 732](#)).
2. To load exchange rate data:
  - If the exchange rate data is specified in a loader file - use the element tags in the following example and substitute the values of the attributes that are listed in the table:

*Table 226. Element tags*

Element	Attribute	Description
exchangeRate	isoCode	A three letter ISO currency code
exchangeRate	rate	The currency exchange rate

The following example loads currency exchange rates for the Canadian dollar (CAD) and Mexican peso (MXN).

```
<?xml version="1.0" encoding="UTF-8"?>
<openpagesConfiguration xmlFormatVersion="1.31">
 <exchangeRates>
 <exchangeRate isoCode="CAD"
 startDate="2018-05-09 17:36:12"
 rate="0.8636"/>
 <exchangeRate isoCode="MXN"
 startDate="2018-05-09 17:36:12"
 rate="0.0951"/>
 </exchangeRates>
</openpagesConfiguration>
```

- If the exchange rate data is contained in a CSV file for upload, use the element tag in the following example to upload a .csv file. Substitute the value of the attribute that is listed in the table:

*Table 227. Element tag to upload a .csv file*

Element	Attribute	Description
uploadFile	name	The file path and name of the CSV file

For example:

```
<uploadFile name="c:\loaders\rate-update1.csv" dataType="Exchange Rates" />
```

3. Use the ObjectManager load command to import the data. See the [“Load command example” on page 734](#).

## Exporting all currency exchange rates

To export (dump) all the currency exchange rates from your system, you must modify some of the settings in the ObjectManager.properties file.

For information about the file, see [“Modifying the ObjectManager properties file” on page 742](#).

### Before you begin

To use this function, the currency must have a standard 3-letter ISO code and exist in your system.

### Procedure

1. In the ObjectManager.properties file:

- a) Set the values of the following properties as shown:

```
configuration.manager.migrate.configuration.objects=false
```

```
configuration.manager.dump.currency.exchange.rates=true
```

- a) Set the dump options for all other objects to false.

2. Use the ObjectManager dump command to export the data. See the [“Dump command example” on page 735](#).

## Enabling and disabling currencies

You can enable one or more currencies to make it available to the appropriate processes, or you can disable one or more currencies from IBM OpenPages with Watson.

A disabled currency can be enabled later.

### Before you begin

To use this function, the currency must have a standard three letter ISO code and exist in your system.

### Procedure

1. Create an XML data loader file (see [“Creating a data loader file” on page 732](#)).
2. To enable or disable one or more currencies, use the element tags in the following example and substitute the values of the attributes that are listed in the table:

*Table 228. Elements to enable or disable currencies*

Element	Attribute	Description
currency	isoCode	A three letter ISO currency code
currency	enabled	If you set the value to: <ul style="list-style-type: none"><li>• true - the currency is enabled</li><li>• false - the currency is disabled</li></ul>

The following example enables Euros and disables United Kingdom pounds.

```
<currencies>
 <currency isoCode="EUR"
 enabled="true"/>
 <currency isoCode="GBP"
 enabled="false"/>
</currencies>
```

3. Use the ObjectManager load command to import the data. See the [“Load command example” on page 734](#).

## Importing currency field definitions

You can import currency field definitions.

### Before you begin

In IBM Db2 environments, before you import an ObjectManager load that contains metadata definitions (such as fields, field groups, object type, object type associations), drop the reporting schema. Then, when the import completes, re-create the reporting schema.

### Procedure

1. Create an XML data loader file (see [“Creating a data loader file” on page 732](#)).
2. To import currency field definitions, use the element tags in the following example and substitute the values of the attributes listed in the table:

*Table 229. Elements for importing currency field definitions*

Element	Attribute	Description
bundleType	name	The name of a field group
bundleType	description	A brief description of the field group
propertyType	name	The name of a currency field within the specified field group
propertyType	description	A brief description of the currency field
propertyType	required	If you set the element to one of the following values: <ul style="list-style-type: none"><li>• true - the field is required</li><li>• false - the field is not required</li></ul>
propertyType	multiValued	If you set the element to one of the following values: <ul style="list-style-type: none"><li>• true - multiple values can be selected from the list</li><li>• false - only one value can be selected from the list</li></ul>

The following example loads the definition for the currency field “testCurrency” that belongs to a group of the same name.

```
<bundleTypes>
 <bundleType name="testCurrency"
 description="Sarbanes-Oxley Self-Assessment system bundle"
 type="Content Type">
 <propertyType name="testCurrency"
 description="Annualized Value may be used to capture the account
balance from operational systems."
 dataType="Currency"
 minValue=""
 maxValue=""
 defaultValue=""
 required="false"
 currencyCode=""
 multiValued="false">
```

```
</propertyType>
</bundleType>
</bundleTypes>
```

3. Use the ObjectManager load command to import the data. See the “[Load command example](#)” on page 734.

## Exporting currency field definitions

To export (dump) currency field definitions from your system, you must modify some of the settings in the ObjectManager.properties file.

For information about the file, see [“Modifying the ObjectManager properties file” on page 742](#).

### Procedure

1. In the ObjectManager.properties file, set the values of the following properties as shown:

```
configuration.manager.migrate.configuration.objects=false
configuration.manager.dump.bundle.types=true
```

**Tip:** When you use ObjectManager to export all object instances and their relationships, and you have a large dataset, ObjectManager will report an exception in ObjectManager.log. To avoid the exception, limit the size of the data that is exported by specifying a folder path or selecting the specific objects in the hierarchy. To specify a folder path, add the following property: configuration.manager.dump.resources.root.folder=folder\_path. To specify multiple objects whose hierarchies are to be exported, add the following property, where number is a positive integer:

```
configuration.manager.dump.associated.resources.root.node.n=number
```

2. Use the ObjectManager dump command to export the data. See the “[Dump command example](#)” on page 735.

## Importing computed field definitions

You can import computed field definitions.

For information on computed fields, see [“Defining a computed field” on page 183](#).

### Before you begin

In IBM Db2 environments, before you import an ObjectManager load that contains metadata definitions (such as fields, field groups, object type, object type associations), drop the reporting schema. Then, when the import completes, re-create the reporting schema.

### Procedure

1. Create an XML data loader file (see [“Creating a data loader file” on page 732](#)).
2. To import computed field definitions, use the element tags in the following example and substitute the values of the attributes listed in the table:

*Table 230. Elements to import computed field definitions*

Element	Attribute	Description
computationHandle `	name	Do not change. A field definition attribute of the computed field.
computationHandle `	value	A value that corresponds to a particular field definition attribute.

The following example loads the definition of a computed field.

```
<computationHandler name="CognosComputationHandler">
 <computationHandlerAttribute name="Equation"
 value="count(distinct
[DEFAULT].[SOXTEST].[TE_TEST_ID])"/>
 <computationHandlerAttribute name="Namespace"
 value="DEFAULT"/>
 <computationHandlerAttribute name="Object ID Column"
 value="Just some text"/>
 <computationHandlerAttribute name="Reporting Period ID
Column"
 value="Value for testing"/>
</computationHandler>
```

3. Use the ObjectManager load command to import the data. See the [“Load command example” on page 734](#).

## Exporting computed field definitions

To export (dump) computed field definitions from your system, you must modify some of the settings in the `ObjectManager.properties` file.

For information about the file, see [“Modifying the ObjectManager properties file” on page 742](#).

### Procedure

1. In the `ObjectManager.properties` file, set the value of the following property as shown:  
`configuration.manager.migrate.configuration.objects=true`

**Tip:** When you use ObjectManager to export all object instances and their relationships, and you have a large dataset, ObjectManager will report an exception in `ObjectManager.log`. To avoid the exception, limit the size of the data that is exported by specifying a folder path or selecting the specific objects in the hierarchy. To specify a folder path, add the following property: `configuration.manager.dump.resources.root.folder=folder_path`. To specify multiple objects whose hierarchies are to be exported, add the following property: `configuration.manager.dump.associated.resources.root.node.n=number`, where `number` is a positive integer.

2. Set the dump options for all other objects to `false`.
3. Use the ObjectManager dump command to export the data. See the [“Dump command example” on page 735](#).

## Exporting file attachments

This example shows how an IBM OpenPages with Watson administrator can export file attachments.

### Procedure

1. Log on to the application server.
2. Edit the `ObjectManager.properties` file. Configure all properties to be `false` except for the following property:

```
configuration.manager.dump.non.form.based.resources=true
```

If you want to limit the export to a specific system folder and its subfolders, set the `configuration.manager.dump.resources.root.folder` property.

For example:

```
configuration.manager.dump.resources.root.folder=/_op_sox_documents/Files and Forms/
Company ABC/SubEntity Folder
```

3. Save the file.

4. Open a command prompt or a shell.
5. Go to the *OP\_HOME/bin* directory where *OP\_HOME* represents the installation location of the OpenPages with Watson application.
6. Run the following command:

```
ObjectManager.cmd|sh d c <user> <password> <file_location> <file_name_prefix>
```

For example, the following syntax creates a file called *ExportedFile-op-file-content.zip* in the C:\TMP directory.

```
ObjectManager d c OpenPagesAdministrator password C:\TMP ExportedFile
```

## Importing file attachments

This example shows how an IBM OpenPages with Watson administrator can import file attachments.

### Procedure

1. Create a .zip file that contains the attachments that you want to import. Name the file *<prefix>-op-file-content.zip*.

**Note:** The zip file must use UTF-8 encoding.

For example: *myfiles-op-file-content.zip*

2. Create an XML loader file. Name the file *<prefix>-op-config.xml*. Use the same *<prefix>* as the .zip file.

For example: *myfiles-op-config.xml*

3. In the *<prefix>-op-config.xml* file, add the following text:

```
<?xml version="1.0" encoding="UTF-8"?>
<openpagesConfiguration>
 <nonFormBasedResources>
 <resource resourceType="Asset"
 shortName="<attachment>"
 name="/_op_sox_documents/Files and Forms/<business_entity>/<attachment>"
 parentFolder="/_op_sox_documents/Files and Forms/<business_entity>"
 contentLocation="/<attachment>"
 description=""
 checkedOut="false"
 checkedOutBy=""
 checkedOutDate=""
 contentLanguage=""
 contentLength="0"
 contentType="SOXDocument"
 creationDate=""
 creator="OpenPagesAdministrator"
 fileType=""
 inheritAcls="true"
 modificationDate=""
 modifiedBy=""
 multiVersionable="true"
 sourceResource=""
 storageServer=""
 subResourceType="Normal"
 visibilityType="Normal" />
 </nonFormBasedResources>
 <resourceSets>
 <resourceSet name="SOX.ProjectDefault" description="SOX.ProjectDefault">
 <resourceNode name="/_op_sox/Project/Default/BusinessEntity/<business_entity>/<business_entity_name>.txt">
 <resourceNodeChild name="/_op_sox_documents/Files and Forms/<business_entity>/<attachment>" />
 </resourceNode>
 </resourceSet>
 </resourceSets>
</openpagesConfiguration>
```

- *<attachment>*: The file name and extension of a file attachment in the *<prefix>-op-file-content.zip* file.

- <*business\_entity*>: The path and name of the parent business entity for the file attachment, for example: /Global Financial Services/Corporate.
- <*business\_entity\_name*>: The name of the business entity for the file attachment, for example / Corporate.

To find the business entity path and name, open the task view for the business entity. The path and name are in the **Folder** field.

The screenshot shows the IBM OpenPages with Watson interface. At the top, there's a navigation bar with icons for Home, Business Ent..., and Corporate. Below it, a title bar says 'Business Entity' and 'Corporate'. A toolbar has tabs for Task (which is selected), Activity, and Admin. There's a search bar and a 'Reveal editable fields' button. On the right, there are status indicators for 'Modified' and 'Required' with a help icon. The main area is titled 'General' with an info icon. It contains fields for Name (Corporate) and Description (Organisational Unit). To the right, there's a 'Folder' field with a yellow background containing the path 'Global Financial Services / Corporate'. Other sections like Entity Type and Jurisdiction are visible at the bottom.

In this example, the attachment is called MyFile.docx and the parent business entity is Global Financial Services/Corporate:

```

<?xml version="1.0" encoding="UTF-8"?>
<openpagesConfiguration>
 <nonFormBasedResources>
 <resource resourceType="Asset"
 shortName="MyFile.docx"
 name="/_op_sox_documents/Files and Forms/Global Financial Services/Corporate/
MyFile.docx"
 parentFolder="/_op_sox_documents/Files and Forms/Global Financial Services/
Corporate"
 contentLocation="/MyFile.docx"
 description=""
 checkedOut="false"
 checkedOutBy=""
 checkedOutDate=""
 contentLanguage=""
 contentLength="0"
 contentType="SOXDocument"
 creationDate=""
 creator="OpenPagesAdministrator"
 fileType=""
 inheritAcls="true"
 modificationDate=""
 modifiedBy=""
 multiVersionable="true"
 sourceResource=""
 storageServer=""
 subResourceType="Normal"
 visibilityType="Normal" />
 </nonFormBasedResources>
 <resourceSets>
 <resourceSet name="SOX.ProjectDefault" description="SOX.ProjectDefault">
 <resourceNode name="/_op_sox/Project/Default/BusinessEntity/Global Financial
Services/Corporate/Corporate.txt">
 <resourceNodeChild name="/_op_sox_documents/Files and Forms/Global Financial
Services/Corporate/MyFile.docx" />
 </resourceNode>
 </resourceSet>
 </resourceSets>
</openpagesConfiguration>

```

```

 </resourceSets>
 </openpagesConfiguration>

```

4. If you want to import multiple file attachments, add a `<resource>` element and a `<resourceNode>` element for each file.

For example:

```

<?xml version="1.0" encoding="UTF-8"?>
<openpagesConfiguration>
 <nonFormBasedResources>
 <resource resourceType="Asset"
 shortName="MyFile.docx"
 name="/_op_sox_documents/Files and Forms/Global Financial Services/Corporate/
MyFile.docx"
 parentFolder="/_op_sox_documents/Files and Forms/Global Financial Services/
Corporate"
 contentLocation="/MyFile.docx"
 description=""
 checkedOut="false"
 checkedOutBy=""
 checkedOutDate=""
 contentLanguage=""
 contentLength="0"
 contentType="SOXDocument"
 creationDate=""
 creator="OpenPagesAdministrator"
 fileType=""
 inheritAcls="true"
 modificationDate=""
 modifiedBy=""
 multiVersionable="true"
 sourceResource=""
 storageServer=""
 subResourceType="Normal"
 visibilityType="Normal" />
 <resource resourceType="Asset"
 shortName="MyOtherFile.xlsx"
 name="/_op_sox_documents/Files and Forms/Global Financial Services/Corporate/
MyOtherFile.docx"
 parentFolder="/_op_sox_documents/Files and Forms/Global Financial Services/
Corporate"
 contentLocation="/MyOtherFile.docx"
 description=""
 checkedOut="false"
 checkedOutBy=""
 checkedOutDate=""
 contentLanguage=""
 contentLength="0"
 contentType="SOXDocument"
 creationDate=""
 creator="OpenPagesAdministrator"
 fileType=""
 inheritAcls="true"
 modificationDate=""
 modifiedBy=""
 multiVersionable="true"
 sourceResource=""
 storageServer=""
 subResourceType="Normal"
 visibilityType="Normal" />
 </nonFormBasedResources>
 <resourceSets>
 <resourceSet name="SOX.ProjectDefault" description="SOX.ProjectDefault">
 <resourceNode name="/_op_sox/Project/Default/BusinessEntity/Global Financial
Services/Corporate/Corporate.txt">
 <resourceNodeChild name="/_op_sox_documents/Files and Forms/Global Financial
Services/Corporate/MyFile.docx" />
 </resourceNode>
 <resourceNode name="/_op_sox/Project/Default/BusinessEntity/Global Financial
Services/Corporate/Corporate.txt">
 <resourceNodeChild name="/_op_sox_documents/Files and Forms/Global Financial
Services/Corporate/MyOtherFile.docx" />
 </resourceNode>
 </resourceSet>
 </resourceSets>
</openpagesConfiguration>

```

5. Put the `<prefix>-op-file-content.zip` and `<prefix>-op-config.xml` files info the same directory.

6. Log on to the application server.
7. Open a command prompt or a shell.
8. Go to the <OP\_HOME>/bin directory where <OP\_HOME> represents the installation location of the OpenPages with Watson application.
9. Run the following command:

```
ObjectManager.cmd|sh l c <admin_user> <admin_password> <file_location> <prefix>
```

For example, the following command imports a file that is called myfiles-op-file-content.zip that is located in the C:\TMP directory.

```
ObjectManager l c OpenPagesAdministrator password C:\TMP myfiles
```

## Migrating configuration changes using the ObjectManager tool

You can use the ObjectManager tool to migrate configuration changes from one deployment environment to another.

The source and target environments must have the same version and patch level of OpenPages with Watson.

### Multi-deployment environments

If you have a multi-deployment environment where changes to the IBM OpenPages with Watson application are tested and validated prior to implementation, you can use ObjectManager, a command line interface (CLI) tool, to migrate configuration changes from one deployment environment to another.

Multi-deployment environments may vary from company to company. For example, a multi-deployment environment for "Company 1" might contain the following deployments:

- Development Deployment - configuration changes are made to the user interface and tested to validate that the changes are applied correctly. The OpenPages with Watson repository used in this deployment might contain fewer objects (partial instance data) than the Production deployment.
- Test Deployment - configuration changes from the Development configuration are imported (to avoid error) and validated through the ObjectManager tool and tested. The OpenPages with Watson repository used in this deployment generally mirrors the instance data in the Production deployment.
- Production Deployment - The tested configuration changes from the Test configuration are imported (to avoid error) and validated through the ObjectManager tool, and then made available to end users (Live Production).

"Company 2" might, for example, combine Development and Test into a single Test deployment before migrating configuration changes to a Production environment.

## The ObjectManager migration process

Using the ObjectManager tool, you can migrate configuration changes from one deployment to another for the following objects:

- Field Groups
- Object Types
- Filters
- Field Dependencies
- Dependent Picklists
- Object Type Relationships
- Profiles
- Application Text

- Object Text
- Settings (excludes machine-specific settings in the IBM OpenPages with Watson repository)
- Rules (from the **Rules Engine**)
- Workflow definitions in GRC Workflow
- Jobs in the Scheduler
- Calculations (from GRC Calculations)
- Solution visualizations

You can also export and import security rules. However, any existing security rules are overwritten by the import. If you want to migrate security rules, export the security rules from the target environment, modify the exported file to add or modify the security rules, and then import the updated file into the target environment.

To limit the scope of the changes to the previously mentioned configuration objects, you can edit settings in the `ObjectManager.properties` file. For more information, see [“Modifying ObjectManager settings” on page 761](#).

[Table 231 on page 761](#) outlines the process that you can follow if you want to migrate configuration changes, for example, from a Test environment to a Production environment.

**Note:** If you have a multi-deployment environment that also includes a Development environment, you can use the tasks that are outlined in [Table 231 on page 761](#) to do an initial export of the configuration data from the Development environment to the Test environment.

<i>Table 231. Tasks for migrating configuration changes</i>		
<b>Use this deployment...</b>	<b>To do this task...</b>	<b>Related topic...</b>
Test	1. Modify settings in the <code>ObjectManager.properties</code> file to limit the scope of the export data to only configuration objects.	See “ <a href="#">Modifying ObjectManager settings” on page 761</a> for step-by-step setup instructions before you export configuration data.
Test	2. Export the configuration changes into a file.	See “ <a href="#">Exporting configuration changes” on page 763</a> for step-by-step instructions on how to export configuration metadata.
Production	3. Compare the configuration changes from the previous deployment (in task 2) against this deployment.	See “ <a href="#">Validating configuration changes” on page 764</a> for step-by-step instructions on how to validate configuration changes.
Production	4. Import the configuration changes (from task 3) into the current deployment.	See “ <a href="#">Importing configuration changes” on page 765</a> for step-by-step instructions on how to update configuration changes.
Production	5. To validate that all the updates were applied, compare the configuration changes from the previous deployment (in task 2) against the newly updated deployment.	See “ <a href="#">Validating configuration changes” on page 764</a> for step-by-step instructions on how to validate configuration changes.

## Modifying ObjectManager settings

Before you begin migrating configuration object changes from one deployment to another, you can use the ObjectManager tool to include only configuration objects in the migration process and exclude additional object data, such as Resource or Job Type data, from the migration metadata and changes.

## **Limiting the export of changes to configuration objects**

By default, the ability to export metadata changes is set to include all objects. So that you can export changes made only to configuration objects, you must modify some of the settings in the ObjectManager.properties file.

### **Procedure**

1. In a text editor of your choice, open the ObjectManager.properties file (see [“Modifying the ObjectManager properties file” on page 742](#)).
2. Navigate to the following setting in the file:  
`configuration.manager.migrate.configuration.objects=false`
3. Change the value of this setting from false (default) to true (export only configuration object changes) as follows:  
`configuration.manager.migrate.configuration.objects=true`
4. When finished, save your changes to the file.
5. If you want to modify IBM OpenPages with Watson repository settings that are excluded, by default, from the migration process, follow the instructions in [“Modifying excluded settings from export” on page 762](#).

## **Modifying excluded settings from export**

If the value of some IBM OpenPages with Watson repository settings were changed to reflect a particular deployment environment, you can optionally exclude these settings from migrating to the next deployment environment.

For example, if the address of the Notification Mail Server differs from the Development machine to the Test machine, you can exclude this setting from the export of configuration metadata and changes.

You can optionally exclude settings from export by modifying the ObjectManager.properties file. A statement that excludes a setting from export has the following syntax:

```
configuration.manager.migrate.configuration.exclude.registry.entry.<n>=<setting>
```

Where:

- <n> is a sequential number.
- <setting> is the full path and name of the setting you want to exclude.

By default, OpenPages with Watson excludes certain configuration settings from the export process. These settings are listed in the ObjectManager.properties file along with their full path and name. For example:

```
configuration.manager.migrate.configuration.exclude.registry.entry.1=/OpenPages/
Applications/Common/Email/Mail Server
```

You can add additional settings to the list for exclusion or remove an existing setting from the list to include it in the export.

### **Procedure**

1. Open the ObjectManager.properties file (see [“Modifying the ObjectManager properties file” on page 742](#)).
2. Locate the following setting in the file - you will use this setting as the basis for creating additional settings for exclusion:

```
configuration.manager.migrate.configuration.exclude.registry.entry.
1=/OpenPages/Applications/Common/Email/Mail Server
```

3. To exclude additional settings from export, copy the line of code in Step 2 and do the following:
  - a) Paste the code at the end of the list (for example, after 21).
  - b) Increment the number (for example, 22).
  - c) Specify a full setting path and name.

For example (do not wrap - use a single line):

```
configuration.manager.migrate.configuration.exclude.registry.entry.
22=/OpenPages/Platform/Reporting Schema/Object URL Generator/Populate Past Periods
```

4. To export a configuration setting that is on the excluded list, remove the line of code for that setting from the list.
5. When finished, save your changes to the properties file.
6. Use the ObjectManager dump command to export the data. See “[Dump command example](#)” on page [735](#). Not all items in the exclude list will be in the XML dump file.

**Note:** Make changes to the exclusion list by editing the ObjectManager.properties file in ObjectManager. Changes to ObjectManager.properties are ignored if you use Environment Migration.

## Disabling triggers when migrating environments

When extracting and restoring environments using ObjectManager, you might need to disable any triggers that are checking data validity. This setting is normally applied automatically, but you can disable triggers if the need arises. This procedure disables all triggers in the system.

### Procedure

1. Access the **Settings** page (see [Chapter 20, “Viewing the Configuration and Settings page,” on page 473](#)).
2. Go to the **Applications > GRCM > Disable Triggers** setting.
3. In the **Value** field, type **true**.
4. Click **Done**.

## Migrating configuration changes

After you modify settings in the ObjectManager.properties file, you can begin the migration process.

Migrating configuration changes from one environment to another involves exporting, validating, and importing the changes.

**Note:** The source and target environments must have the same version and patch level of OpenPages with Watson.

### Exporting configuration changes

Exported data represents a snapshot of the configuration objects in the IBM OpenPages with Watson repository for a particular deployment.

When you export configuration changes, you specify a file path and prefix for the file name in the command line. When the data is exported, the ObjectManager tool automatically appends -op-config.xml to the file name prefix to complete the file name.

For example, if you specify the myconfig prefix in the command line for the file name, it results in this file name: myconfig-op-config.xml.

### Procedure

1. Verify that the OpenPages with Watson application is running.

2. Open a command or shell window and change to the <OP\_HOME>/bin directory of your OpenPages with Watson installation.
3. From the command or shell window, run an ObjectManager command on a single line.
  - a) On a computer running a Microsoft Windows operating system:

```
ObjectManager dump config <admin-user> <password> <config-folder-path> <prefix>
```

- b) On a computer running a Linux operating system:

```
./ObjectManager.sh dump config <admin-user> <password> <config-folder-path> <prefix>
```

Where:

- <admin-user> is the user name of the Super Administrator account (for example, OpenPagesAdministrator).
- <password> is the password of the Super Administrator account.
- <config-folder-path> is the file path to the folder where the exported file will reside. If the folder does not already exist, ObjectManager will create it.
- <prefix> is the prefix for the file name that will be used by ObjectManager.

For example, on a Windows operating system:

```
ObjectManager dump config OpenPagesAdministrator password c:\temp myconfig
```

4. To compare the exported configuration data against the configuration data in the OpenPages with Watson repository of the next deployment environment, see “[Validating configuration changes](#)” on page 764.

## Validating configuration changes

After you export or import configuration changes, you can compare the exported data file from the previous deployment environment against the data in the IBM OpenPages with Watson repository of the current deployment environment.

When you run the validate command by using the ObjectManager tool:

- The results are displayed on the screen during the validation process. If you want to review the results at a later time, you can re-direct the screen output to a file.
- An ObjectManager.log file that contains exception errors is created. This log file is located in the <config-folder-path> directory.

## Procedure

1. Copy the exported configuration file from the previous deployment environment (for example, Development) to a folder in the current deployment environment (for example, Production).
2. From the <OP\_HOME>/bin directory of your OpenPages with Watson installation, open a command or shell window.
3. From the command or shell window, run an ObjectManager command on a single line (optionally re-direct the output to a file):

- a) On a computer running a Microsoft Windows operating system:

```
ObjectManager validate config <admin-user> <password> <config-folder-path> <prefix>
```

- b) On a computer running a Linux operating system:

```
./ObjectManager.sh validate config <admin-user> <password> <config-folder-path> <prefix>
```

Where:

- <*admin-user*> is the user name of the Super Administrator account (for example, OpenPagesAdministrator).
- <*password*> is the password of the Super Administrator account.
- <*config-folder-path*> is the file path to the folder where the exported file will reside. If the folder does not already exist, ObjectManager will create it.
- <*prefix*> is the prefix for the file name that will be used by ObjectManager.

On a Windows operating system, the command in the following example compares configuration data in the export file myconfig-op-config.xml located in the c :\temp folder to configuration data in the current deployment, and redirects the display output (from a Windows server) to a text file called config\_log.txt also located in the c :\temp folder:

```
ObjectManager validate config OpenPagesAdministrator password c:\temp myconfig
>c:\temp\config_log.txt
```

4. Review the output for any errors.
5. To import the configuration changes and update the repository of the current deployment environment with these changes, see “[Importing configuration changes](#)” on page 765.
6. To validate that the updated repository of the current deployment matches the configuration changes from the export file, repeat Steps 2-4.

## Results

Validation errors indicate a problem with the data itself and should be corrected before importing the configuration changes into the next deployment. The following sample validation error shows the name field in the export file as having an empty value.

VALIDATION ERROR (Line: 104481 Column: 57): Attribute 'name' is either empty or not provided.

Verification errors indicate differences in the content of the configuration data between the export file and the OpenPages with Watson repository. The following sample verification error shows a discrepancy in the display label text for the Control Method object field between the export file of the previous deployment (Control Method) and the OpenPages with Watson repository of the current deployment (Implementation Method).

VERIFICATION ERROR (Line: 104873 Column: 52): Attribute 'singularValue' for element 'fieldString'(Control Method) did not verify. XML Value: <Control Method> OPX Platform Value: <Implementation Method>.

When the processing is complete, a summary of the configuration objects that were processed is displayed.

After the repository is updated with the configuration changes from the export file and the validation process is repeated, the data in the export file and in the repository should match and no errors should be displayed.

## Importing configuration changes

After comparing and validating the configuration metadata and changes, you can migrate the changes to the current deployment environment or system.

When you import the configuration changes from the previous deployment, the configuration objects in the IBM OpenPages with Watson repository of the current deployment are updated with those changes.

**Note:** The source and target environments must have the same version and patch level of OpenPages with Watson.

An alternative to using the command-line interface (CLI) tool in ObjectManager is to use  > **System Migration** > **Import Configuration** to import the XML file. For information, see “[Importing a migration file](#)” on page 729.

## Procedure

1. Verify that the OpenPages with Watson application is running.
2. Open a command or shell window and change to the <OP\_HOME>/bin directory of your OpenPages with Watson installation.
3. From the command or shell window, run an ObjectManager command on a single line:
  - a) On a computer running a Microsoft Windows operating system:

```
ObjectManager load config <admin-user> <password> <config-folder-path> <prefix>
```

- b) On a computer running a Linux operating system:

```
./ObjectManager.sh load config <admin-user> <password> <config-folder-path> <prefix>
```

Where:

- <admin-user> is the user name of the Super Administrator account (for example, OpenPagesAdministrator).
- <password> is the password of the Super Administrator account.
- <config-folder-path> is the file path to the folder where the exported file will reside. If the folder does not already exist, ObjectManager will create it.
- <prefix> is the prefix for the file name that will be used by ObjectManager.

For example, on a Windows operating system:

```
ObjectManager load config OpenPagesAdministrator password c:\temp myconfig
```

4. To see the configuration changes in the application, stop and then restart the OpenPages with Watson application services.
5. To validate that the newly updated OpenPages with Watson repository matches the configuration changes from the export file, see the topic “[Validating configuration changes](#)” on page 764.
6. To export the configuration data to a file, see the topic “[Exporting configuration changes](#)” on page 763.

## What to do next

If you loaded profiles, update the reporting schema. For more information, see “[Updating the reporting schema](#)” on page 121.

---

# Chapter 28. Using FastMap

FastMap is a productivity tool that works with the IBM OpenPages with Watson export feature, and automates the importing and batch processing of object data into OpenPages with Watson.

The FastMap tool uses a data load template (a Microsoft Excel workbook in .xlsx format) to capture data for import. When you import data into OpenPages with Watson, FastMap validates the data and, if no errors are found, populates the repository with the new or updated records.

## Sample scenario

You have 150 Process and 175 Risk objects (records) that require either creation or updating. Rather than manually creating or updating individual Process and Risk objects through the OpenPages with Watson application interface, you use a FastMap data load template to capture the data for batch processing.

After the data is captured, log on to the OpenPages with Watson application and import the template (in .xlsx format) through FastMap for validation. During the validation phase, you receive a few validation errors. You fix the errors in the template and resubmit it. This time, no validation errors are reported and the data is automatically processed. After processing is complete, the objects become available for reports and updating by users.

This video demonstrates how to use FastMap to import data:

<https://youtu.be/iv9cK3yqtxc>

## FastMap overview

---

This topic provides an overview of the tasks using FastMap to import data into IBM OpenPages with Watson.

**Note:** FastMap import is not supported for File and Signature objects or for the system Comment field.

The FastMap tool validates and imports object data.

When you import an object using FastMap, the imported object fields are determined by the fields in the applicable **Admin** view. If there is no applicable **Admin** view, FastMap import uses the profile fields.

The following fields are not imported:

- Any field set to **Read only** in the **Admin** view for the object
- Any field not in the **Admin** view for the object
- Any field included in the **Other fields** section of the **Admin** tab for the object

Field dependency rules are not evaluated for FastMap imports. This allows FastMap users to stage data, requiring users to enter required data during subsequent updates.

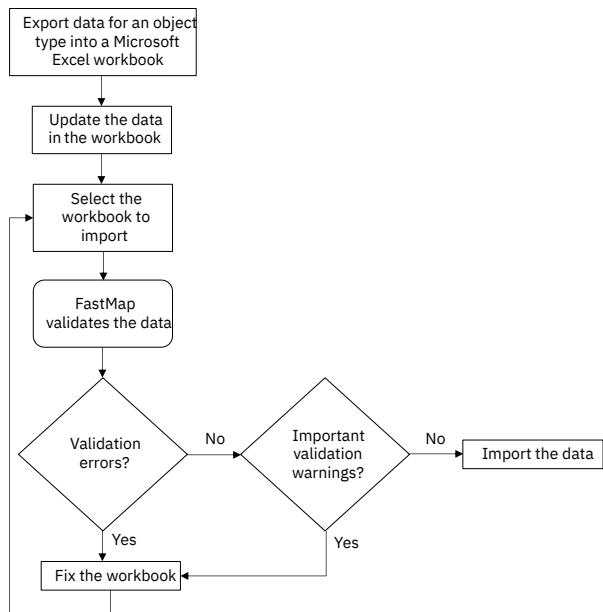


Figure 68. FastMap task flow

## The FastMap import process

The following steps provide an overview of the process for creating and using a FastMap template to import data.

### Procedure

1. To create a Microsoft Excel workbook, select the items you want to modify and export them.
  - Open a grid view. You can use a filter to show only the items you want to export. To export all visible items, click .
  - To export specific items in the grid view, select the checkboxes to the left of each item that you want to export. A different toolbar is displayed. In that toolbar, click .
2. In the **Export** dialog box, select any descendant object types you want to export. Click **Export**. This creates the Microsoft Excel workbook containing the object data.
3. Add or modify the object data in the workbook as needed. Unhide columns if necessary.
4. Optional: Add or modify parameters on the Definition worksheet as needed.  
For more information, see “[Using the FastMap Definition worksheet](#)” on page 783.
5. Save the file.
6. Import the workbook. For more information, see “[Accessing FastMap to import data and view status](#)” on page 770.

## FastMap templates

A FastMap template is a Microsoft Excel workbook with data load worksheets that you can modify.

A workbook for FastMap import has the following characteristics:

- The file must be in .xlsx format.
- Contains one or more data load worksheets.
- Has only one data load worksheet per object type.

- By default, is in the user's locale.
- Optionally, includes a Definition worksheet in a workbook to configure FastMap import and export behavior.

A data load worksheet within a workbook has the following characteristics:

- Is specific to an object type.
- Has a variety of columns where you specify parent and folder paths and change data for listed objects.
- Each column must have a heading name.
- Optionally, includes one or more special column headings.
- Must contain localized column names and data.

## **Example**

You want only users who are assigned the "Upload Data" profile to import changed or new data for the following five object types: Business Entities, Processes, Risks, Controls, and External Losses. You could either create a workbook with multiple worksheets—one for each object type for a total of five data load worksheets, or multiple workbooks—one for each object type.

### **Note:**

- You cannot import attachments or signatures with FastMap.
- FastMap supports the Microsoft Office .xlsx format.
- User access is based on the role template assigned to a user or group. For details about role templates, see ["Role templates" on page 75](#).
- For Long String data types, the medium text subtype is the only subtype supported for FastMap uploads. Fields with a large subtype are ignored by Excel and FastMap as these fields might be too large for Excel to store in a cell (the maximum storage for a cell is 32 KB).
- Fields that cannot be modified, such as the system **Creation Date**, **Created By**, or **Last Modified By** fields, also cannot be edited by using the FastMap process. For example, if you are migrating data, you cannot preserve the creation date information by using FastMap. FastMap import is not supported for the system Comment field.

## **The FastMap data validation process**

When a FastMap template is imported into the IBM OpenPages with Watson application, FastMap checks the user profile, and the setup and format of the worksheets.

By default, FastMap uses the profile of the logged-on user to determine which object types and fields are valid. For example, if an object type or certain object fields are included in a data load template but are excluded in a user's profile, then that object type or those object fields will be excluded from the data imported by FastMap.

You can override the default profile used by FastMap by explicitly specifying a profile in the Definition worksheet of a template. For example, if you specify the `profileName` parameter as `OpenPages Platform 3`, Fast Map will use that profile when importing data.

In general, FastMap uses the same validation rules that apply to data that is manually entered into the application. For example, validation errors would occur if the profile of the logged-on user includes required fields that are missing from the worksheet, or the maximum number of characters allowed for a field is exceeded, and so forth.

For more details about validation, see ["Resolving FastMap validation errors" on page 771](#).

## **FastMap localization**

By default, FastMap uses the locale of the logged-on user to validate data in templates.

As a result, all data in FastMap templates, such as column headings, text, enumerated drop-down or multivalued selection field values, should be localized in the locale of the end user. For example, an end user with the Italian locale (`it_IT`) setting should only import FastMap templates with localized Italian values.

You can override the locale of the end user by explicitly specifying a locale in the Definition worksheet of a template. For example, if you specify the `locale` parameter as `en_US` and localize the template in English, the Italian user could upload the template for validation in English, not Italian. For more information, see [“Using the FastMap Definition worksheet” on page 783](#).

When you export object type data from the IBM OpenPages with Watson application, the locale is automatically set on the Definition worksheet.

Validation messages that are displayed by FastMap during processing can be localized through application strings.

## Accessing FastMap to import data and view status

---

You can access FastMap to import data or check the status of your data imports. Importing object data using FastMap is a two-step process consisting of validation and importing.

### Before you begin

To access **FastMap Import**, you must have the correct application permission set on your account. For more information about FastMap permissions, see [“Types of application permissions” on page 52](#).

### Procedure

1. Click  > **FastMap Import**.

The **FastMap Import** tab displays a list of your imports. If you have the application permission to see imports performed by other users, you can click the **View** dropdown and select **All imports**. The **Created By** column is added to the grid if you select this view.

2. On the **FastMap Import** tab, click **Import**.
3. In the **FastMap validate and import** dialog box, click **Choose file** and select a file to import.
4. Click **Validate**.

You can either wait for the validation to complete or click **Close, we'll notify you** to be notified when the validation is complete. The notification contains a link to review the validation status messages. If you miss a notification message, you can click **View notification**  to see the message.

### Results

If the validation fails, you are prompted to upload a corrected file.

If the validation completes with warnings, you have the following choices:

- You can upload a corrected file.
- If the warnings don't matter, you can import the object data.
- You can cancel and start the process from the beginning.
- You can close the dialog box. Later in the current session, you can view the notifications to see the list of warnings or return to the **FastMap Import** tab to import the file.

When validation completes successfully, you can choose to import or cancel.

When you choose to import, the progress indicator updates automatically. You can close the **FastMap import details** dialog box at any time and you will be notified when the import is complete.

## Resolving FastMap validation errors

Before FastMap can import data into the IBM OpenPages with Watson application, all validation errors that are displayed in the FastMap validation dialog box must be resolved.

You resolve these errors by opening the FastMap template in Microsoft Excel and modifying the data.

When finished, you must resubmit the updated template to FastMap for another validation check. If errors are still found, you must repeat the resolution process until all validation errors are resolved. After all validation errors are resolved, FastMap is ready to import the data into the OpenPages with Watson application.

## Understanding FastMap validation errors

Validation errors and warnings are displayed in the FastMap validation dialog box after validation completes.

If the FastMap validation process completes with:

- No validation errors - a status message is displayed indicating the number of objects to be imported.
- Warnings - you can load your data or correct the warnings and revalidate.
- Errors - a "Validation Failed" status is displayed along with information about the error.

[Table 232 on page 771](#) lists some of the most common messages that may be displayed in a FastMap Import window.

Table 232. FastMap import validation error information		
This column...	Displays this...	Possible values...
Type	The category of the message.	<ul style="list-style-type: none"><li>• Error</li><li>• Warning</li></ul>
Description	The type of error, and the name of the missing or invalid object field or invalid value.	<a href="#">See "Troubleshooting FastMap validation messages" on page 772.</a>
Sheet	The name of the object type worksheet.	For example, Processes or Risks.
Row	The row within the Excel worksheet containing the error.	The index number corresponding to a row, for example, 2.
Column Index	The column index within the Excel worksheet containing the error.	The index letter corresponding to a column, for example, N.
Column Header	The name of the column within the Excel worksheet containing the error.	The localized label of a field name, for example, Domain.

For example, if the following validation message was displayed in the table on the FastMap Import window:

```
Error Required property is missing value.(Domain) Processes 2 N Domain
```

You would open the data load template, and enter the missing value (such as Financial Management) in row 2 under the Domain column (N) on the Processes worksheet.

## Troubleshooting FastMap conflict with recent updates warning message

If you are unable to import changes and this warning message is displayed: Record conflicts with more recent updates and will be ignored. You need to check the timestamp value for the exportDate parameter on the Definition worksheet in the template. The warning message is displayed

whenever you try to import a template and the data for an object has been updated since the specified export timestamp.

**Important:** If you are certain that the changes you want to import are current for all objects in the workbook, you can remove the export timestamp from the template following this procedure.

## Procedure

1. Open the FastMap template in Excel.
  - a) If necessary, unhide the Definition worksheet (see [“Unhiding a FastMap Definition worksheet” on page 784](#)).
  - b) Remove the exportDate parameter.
  - c) Save the change.
2. Resubmit the template for import.

## Troubleshooting FastMap validation messages

FastMap Validation Messages contains a list of FastMap validation messages, a brief description of the cause of the message, and what a user can do to resolve the issue.

In the following two tables, [Table 233 on page 772](#) and [Table 234 on page 776](#), messages are listed in alphabetical order.

Table 233. FastMap validation error messages		
Message	Cause	Resolution
Currency field is missing currency code.	A local amount is entered but the Local Code field is blank.	Make sure a value is set for Local Code in currency fields.
Currency field is missing local amount.	A local code is entered but the Local Amount field is blank.	Make sure a value is set for Local Amount in currency fields.
Exchange rate for base currency can only be set to 1.	The Local Code and Base Code fields are set to the same value but the Exchange Rate field is set to a value other than 1.	If the Local Code and Base Code values are the same, set the Exchange Rate field to a value of 1.
Import of Signature Objects not supported.	Signature objects are not supported for import.	Remove Signature objects from the worksheet.
Invalid boolean format. Value must be either true or false.	An invalid Boolean value is specified.	Ensure the Boolean value is set to either true or false.
Invalid classifier format.	Values in classifier fields or classifier target fields were exported, edited, and re-imported.	Remove the value from the spreadsheet or re-export and import the data. Do not edit classifier fields or classifier target fields after exporting them.
Invalid currency code.	An invalid value was entered for a currency code.	Ensure the 3-letter ISO currency code is spelled correctly and is valid.

Table 233. FastMap validation error messages (continued)

Message	Cause	Resolution
Invalid date format.	The cell contents for a Date field are not recognized.	Format the cell in Excel as Date to resolve the issue.  If you leave the format as either General or Text, the text in the cell must match the inputDateFormat parameter. You can set this on the Definition worksheet to values such as dd/mm/yy.
Invalid decimal format.	A non-numeric value was entered for a decimal field.	Make sure that decimal fields have a numeric value.
Invalid decimal range.	The numeric value entered is outside the minimum or maximum range defined for that field.	Make sure the specified value is within the numeric range defined for that field.
Invalid Exchange Rate.	Exchange rate is 0 or negative.	Make sure the exchange rate value is greater than 0 (zero).
Invalid group.	An invalid value was entered for a Group field.	Ensure the name of the group is spelled correctly and is valid.
Invalid Integer format	A non-numeric value was entered for a numeric value.	Make sure the field has a numeric value.
Invalid Integer range.	The numeric value entered is outside the minimum or maximum range defined for that field.	Make sure the specified value is within the numeric range defined for that field.
Invalid Object Profile. Unable to properly validate spreadsheet.	A value for the profile is specified that is not recognized.	Ensure the name of the profile is spelled correctly and is valid.
Invalid parent resource provided.	The value of the parentResource parameter is invalid.	Make sure the full path of the specified parent object is correct.
Invalid Property Type.	The column header is not recognized as a property by FastMap.  Possible causes: <ul style="list-style-type: none"><li>• The field is misspelled in the column heading on the worksheet</li><li>• The field is missing from the view of the profile being used to import data. The view is specified by viewName on the Definition worksheet. The default is Admin.</li></ul>	Ensure the column header is spelled correctly. If so, make sure the property is present in your profile's Admin view.  <b>Note:</b> If you do not want the column to be processed, you can list it under the ignoreColumns parameter on the Definition worksheet.
Invalid URL.	An invalid URL was entered for a URL field.	Ensure the URL is correct and fully qualified.
Invalid user.	An invalid value was entered for a User field.	Ensure the name of the user is spelled correctly and is valid.
Invalid user/group.	An invalid value was entered for a User/Group selector.	Ensure the name of the user or group is spelled correctly and is valid.

Table 233. FastMap validation error messages (continued)

Message	Cause	Resolution
Locale is invalid.	The locale value specified is not recognized.	Ensure the value of the locale is spelled correctly and is valid.
Missing currency code column.	The local code column is missing and a local amount is specified.	Make sure the local Currency code column is present in your worksheet and has a value for this record.
Missing local amount column.	The local amount column is missing and a local code is specified.	Make sure the local Amount column is present in your worksheet and has a value for this record.
Multiple resources found with the same key value.	When using Key fields, a key is specified that is not unique and FastMap cannot determine which resource to update.	Make sure the value specified for each Key is unique.
Name cannot be blank.	<ul style="list-style-type: none"> <li>• An object type that is not configured for autonaming has an empty Name.ID or Name field.</li> <li>• The Name.ID or Name column is missing from the worksheet.</li> <li>• The source environment does not use the System Fields:Name.Title field but the target environment does. When the Title field is disabled, the worksheet uses a Name column. When the Title field is enabled, the worksheet uses Name.ID and Name.Title columns.</li> </ul> <p><b>Note:</b> This error will not occur if autonaming is enabled for an object type.</p>	<p>Make sure the Name the column is present in your worksheet and has a value in it for this record.</p> <p>If your target environment uses the Title field, make sure the worksheet contains the Name.ID and Name.Title columns and that the Name.ID field has a value.</p>
Name contains illegal characters.	Name contains backslashes or forward slashes.	Remove any backward slash (\) or forward slash (/) marks from the name of the object.
Name exceeds maximum characters (in bytes).	Name is longer than 252 characters or bytes for multicode locales.	Make sure the name of the object is shorter than 252 characters or bytes.
Object cannot be associated to a parent of this type.	A parent-child relationship does not exist between the object types being associated.	Either enable an association between the object types you want to associate or modify the worksheet to reflect object types that have a child-parent association already configured.
Parent not specified.	<p>A parent is not specified for a new object and the allowOrphans setting is not set to true.</p> <p>Objects being updated do not need to have a parent specified.</p>	Ensure that all three parent fields are present and populated correctly.

Table 233. FastMap validation error messages (continued)

Message	Cause	Resolution
Parent Resource content type not recognized. Check that it is viewable in your profile.	The object type of the resource specified by the parentResource parameter is not recognized.	Ensure the object type value is spelled correctly. If so, make sure the object type is present in your profile's Admin view.
Parent Resource not found.	A parent is specified in your spreadsheet, but FastMap cannot find it in the IBM OpenPages with Watson repository.	Make sure that the Parent Path is pointing to the proper folder location and that the Parent Objects value is the proper name of the object.
Property value exceeds maximum characters.	A text field contains more characters than is allowed in the OpenPages with Watson application.	Modify the text field so it does not exceed the character or byte limit.
Required property is missing value.	A required field for the object type is missing a value.  Possible causes: <ul style="list-style-type: none"><li>• The column is present on the worksheet and the cell is missing a value</li><li>• The column for the required field is missing.</li></ul>	Make sure that you have a value set for all properties required on the object.
System error.	Any unexpected error occurred. Similar to a "Requested operation could not be completed" system error message.	Contact IBM OpenPages Support.
Text field formatted as number in spreadsheet.	A text property value is formatted as a number or a date in the spreadsheet.  A Text field in OpenPages with Watson is formatted in the worksheet cell as Number or Date.  The field cannot be read in by OpenPages with Watson in this state and maintain all of the Excel formatting.	Change the format of the cells in Excel to Text.
The file exceeds the maximum number of rows allowed for import.	The total number of rows in the workbook is greater than the value set in the Maximum Workbook Rows setting (see " <a href="#">Limiting the rows for import to optimize FastMap performance</a> " on page 795).	Modify the worksheet so it does not exceed the row limit or change the value of the setting.
The value entered is not a valid selection for this field.	The value for a single select drop-down field is not a valid value.  The value must be in the proper locale of the user for it to be recognized.	Ensure the value is typed correctly and is in the correct locale.

*Table 233. FastMap validation error messages (continued)*

Message	Cause	Resolution
The value(s) entered are not valid selections for this field.	The value for a multi-select drop-down field is not a valid value.  The value must be in the proper locale of the user for it to be recognized.	Ensure the value is typed correctly and is in the correct locale.

*Table 234. FastMap validation warning messages*

Message	Cause	Resolution
Full import will result in objects being deleted.	When setting fullImport to 'true', FastMap identifies objects to be deleted.	Informational message, no action required.
Invalid Content Type	<p>The worksheet name is not recognized by FastMap as a valid object type in the system.</p> <p>Possible causes:</p> <ul style="list-style-type: none"> <li>The object type is misspelled on the worksheet tab.</li> <li>The object type is missing from the profile being used to import data.</li> </ul> <p>Although FastMap will import the workbook, the invalid worksheet will be ignored.</p> <ul style="list-style-type: none"> <li>In an English locale, the data was exported to Excel. Afterwards, the locale in the Excel worksheet was change to something other than en_US. An error is issued when the data is imported with FastMap.</li> </ul>	<p>Make sure that the object type is spelled correctly on the tab of the worksheet.</p> <p>FastMap treats each worksheet in the workbook as a content type sheet.</p> <p><b>Note:</b> If you do not want the worksheet to be processed, you can list it under the ignoreSheets parameter on the Definition worksheet.</p>
Property is read only.	<p>A value was entered for a field that is read-only in the view of the profile used for import. The view is specified by viewName on the Definition worksheet. The default is Admin.</p> <p>Although FastMap will import data, the read-only field will be ignored.</p>	<p>Remove the columns from your worksheet.</p> <p>You can also specify the ignoreReadOnlyWarnings parameter so that these messages do not occur. However, these fields will not be updated when importing.</p>
Record conflicts with more recent updates and will be ignored.	A record's last modified date is more recent than the value from the exportDate parameter.	See " <a href="#">Troubleshooting FastMap conflict with recent updates warning message</a> " on page 771 for details.

## Creating FastMap import templates

The quickest way to create a FastMap data load template is to export data for an object type into a Microsoft Excel workbook.

You can use that workbook to modify the data, and then use FastMap to import the modified data into the IBM OpenPages with Watson application.

## The data exported to a workbook by FastMap

When you export object data, the resulting Microsoft Excel workbook has the following characteristics:

- Object fields that are displayed in an object's Admin View are exported to a corresponding worksheet in the workbook. However, fields that are included in the **Other fields** section of the **Admin** tab don't appear when doing a FastMap export.
- Each object field is represented by a column on the worksheet.
- FastMap exports fields in the order they appear in the Admin View of the object. If no Admin View exists, fields are not exported in any specific order.
- The header row in the worksheet contains labels for each object field. However, if the `useSystemNames` export template parameter is set to TRUE or if duplicate labels exist in the current locale, there are two header rows. The first header row contains full system names in the format, `<Field Group>.<Field Name>`, and the second header row contains labels for each object field.

For information about the `useSystemNames` export template parameter, see [“FastMap parameters for importing and exporting data” on page 786](#).

- The plural label of the exported object type is displayed on the worksheet tab in the workbook.

**Note:** For compatibility with Microsoft Excel, FastMap removes the following special characters from a plural label on the worksheet tab:

/ \ ? \* : [ ]

For example, if the localized plural label of Risk object types is `/Risks10*`, the tab on the exported worksheet would be `Risks10`.

- Text fields are exported to Microsoft Excel as text cells.
- In the default (out-of-the-box) IBM OpenPages with Watson export template the special Delete column and the three Parent columns are hidden on the object type worksheet.

See [Table 235 on page 778](#) for details.

- The Definition worksheet is included in the workbook and populated, by default, with the `profileName`, `locale`, `exportDate`, and `ignoreReadOnlyWarnings` parameters.

See [“Using the FastMap Definition worksheet” on page 783](#) for details.

## FastMap exported spreadsheet file name characters

When you export object data for an object type, the file name of the exported spreadsheet is derived from the plural label of the object type. If the plural label of the object type contains special characters, these special characters may be removed from the spreadsheet file name by the operating system causing a mismatch between the object type label and the file name. Special characters in a file name are constrained to characters allowed by the operating system.

For more information, see "Rules for Naming Folders and Files" in the *IBM OpenPages with Watson User Guide*.

For additional information about special characters in the exported spreadsheet, see [“The data exported to a workbook by FastMap” on page 777](#).

## Working with data load worksheets

A data load worksheet for an object type contains columns that identify the path and fields of objects (resources) of the same type for which you want to import change data into the IBM OpenPages with Watson application.

### Defining paths for objects

Sample Worksheet for Process Objects lists the various worksheet columns that you use to define the path of an object.

- The path columns in [Figure 72 on page 782](#) must precede any object field columns that are listed in a worksheet.
- If you have set the `parentResource` parameter on the Definition worksheet, the columns in [Figure 72 on page 782](#) are optional.

*Table 235. Columns that define the path of an object*

This column...	Contains...
Folder Path	The path of an object.
Parent Path	The path of an object's parent folder.
Parent Object Types	The type of parent object to which the child object will be associated.
Parent Objects	The name of the parent object.

For a sample worksheet showing these columns, see [“Sample Processes worksheet” on page 781](#).

## Using special column headings

You can add special column headings to a FastMap data load worksheet to:

- Delete objects from the IBM OpenPages with Watson repository (see [“Deleting objects with FastMap” on page 778](#))
- Disassociate objects (see [“Disassociating objects with FastMap” on page 779](#))

**Note:**

- Adding a special column heading to a worksheet is optional.
- The special column headings and values must be localized.
- The values associated with special column headings are not case-sensitive.
- Special column headings can be placed anywhere in a worksheet. Placing these columns at the beginning of a worksheet makes them easy to find later.

## Deleting objects with FastMap

To delete objects from the IBM OpenPages with Watson application, add a Delete column to the data load worksheet.

To delete objects by using FastMap, first ensure that the **Common > Cascade Delete > Include Object Types** setting specifies at least one object type.

By default, the Delete column is present on the worksheet when data is exported from the OpenPages with Watson application. To see how the Delete column is used in an example, see [Figure 70 on page 782](#).

*Table 236. Delete Column Values*

If the value is set to...	Then...
Y	Objects that are specified for deletion (that is, have a Y in their row under the Delete column) will be deleted from the OpenPages with Watson repository. Any objects associated with the specified object using the <b>Cascade Delete &gt; Include Object Types</b> setting will also be deleted from the repository.  After an object is deleted, it cannot be restored.
N or "blank" (no value specified)	The object will not be deleted.  This value is set by default.

[Table 236 on page 778](#) shows the values for the Delete column.

## Disassociating objects with FastMap

To disassociate objects within the IBM OpenPages with Watson application, add a Remove Association column to the data load worksheet.

See [Figure 70 on page 782](#) for an example.

Table 237. Remove Association Column Values	
If the value is set to...	Then...
Y	<p>Child objects with a Y in their row under the Remove Association column will be disassociated from the specified parent object.</p> <p>A parent object is defined by placing information in the corresponding row of the child object for the following columns:</p> <ul style="list-style-type: none"><li>• Parent Path</li><li>• Parent Object Types</li><li>• Parent Objects</li></ul>
N or "blank" (no value specified)	<p>The object will not be disassociated.</p> <p>This value is set by default.</p>

[Table 237 on page 779](#) shows the values for the Remove Association column.

## Defining property fields for objects in FastMap templates

The number and type of object field columns in a FastMap template for an object type are optional and depend on the type of data you want to import.

Here are some general rules for defining object fields:

- Each object field that you want to update for a selected object type requires a separate column on the worksheet.
- You must use localized column names and values.
- All object field columns follow the path definition columns as described in [Table 235 on page 778](#).

For more information about working with object fields, see [“Guidelines for entering object data into FastMap templates” on page 779](#).

## Guidelines for entering object data into FastMap templates

The following are some general rules you should follow when entering object data into a FastMap data load template.

### Associating child objects

To associate child object to parent objects, use the following columns:

- Parent Object Types - This localized column identifies the type of parent to which you are associating the record. For example, Business Entity or Risk.
- Parent Objects - This localized column identifies the name of the parent object to which you are associating the record.

## Naming objects

If the System Fields:Name.Title field is enabled for an object type, FastMap expects the worksheet to include Name.ID and Name.Title columns.

If the System Fields:Name.Title field is not enabled for an object type, FastMap expects the worksheet to include a Name column.

## Auto-naming

FastMap can override auto-naming. If auto-naming is enabled for an object and the Name column is excluded or left blank, the system assigns a name. If auto-naming is enabled for an object and a value exists in the Name.ID or Name column, that value is imported as the name.

## Currency fields

For each currency field that you include in your template, you must use a special column syntax that defines the local currency code, the amount, and exchange rate of that currency data.

Where:

<field name> in [Table 238 on page 780](#) represents the name of a currency field for a specified object.

Table 238. Column syntax for currency fields	
Use this column syntax...	To define...
<field name>.Amount	The amount based on the local currency code.
<field name>.Currency	The local currency code of the data being entered.
<field name>.Exchange Rate	<p>The exchange rate to apply when calculating the value in the System Base Currency.</p> <p><b>Note:</b></p> <ul style="list-style-type: none"><li>This field is optional.</li><li>If an exchange rate is not specified in the template or if the exchange rate is read-only in the profile, it will use the default exchange rate set in the application.</li><li>When entering data where the Local Currency Code is the same as the System Base Currency Code, this column should not be populated.</li></ul>

**Note:** If the following currency-related fields are included on a worksheet, these fields will be ignored during import:

Base Amount (this is a derived value)

Base Code (this value is set globally)

## Enumerated multivalued selection fields

When entering data for enumerated drop-down or multivalued selection fields, only localized values are valid.

Each selection value should be entered on a separate line within the same worksheet cell.

**Note:** To enter data for multiple values in the same worksheet cell, press the Alt+Enter keys simultaneously on your keyboard (after you type the value) to enter a Microsoft Excel line break.

For example, you have a multivalued enumerated field called "Domain" with the following selection values: Compliance, Operational, Technology, Financial Management, Internal Audit. [Figure 69 on page 781](#) shows how data containing multiple values for the "Domain" field might look in the worksheet.

M	N	O
	Domain	
	Compliance	
	Compliance	
	Internal Audit	
	Operational	
	Technology	
	Financial Management	
	Internal Audit	
	Compliance	
	Operational	
	Technology	
	Financial Management	
	Technology	

Figure 69. Sample Multivalued Selection Column with Values

## Adding custom columns and worksheets to FastMap templates

You can add user-defined columns to a worksheet or user-defined worksheets to FastMap templates.

Each custom column that you add to a worksheet must have a heading name, and each custom worksheet that you add to a workbook must have a worksheet name.

So that FastMap does not try to validate any user-defined columns or worksheets, you must add the following parameters to the Definition worksheet:

- ignoreColumns - use for any user-defined columns and specify each heading name. For example, "column1;column2".
- ignoreSheets - use for any user-defined columns and specify the worksheet names. For example, "sheet1;sheet2".

See ["Using the FastMap Definition worksheet" on page 783](#) for a sample Definition worksheet, and ["FastMap parameters for importing and exporting data" on page 786](#) for additional parameters.

## Sample Object worksheet for updating and creating objects

The sample Processes worksheet in [Figure 70 on page 782](#) and Risks worksheet in [Figure 71 on page 782](#) contain a combination of existing objects for update and the creation of new objects.

### Sample Processes worksheet

The sample Processes worksheet in Sample Processes Worksheet shows the following:

- Column A, row 5 contains an existing Process object (Proc-B03) that will be disassociated from the Boston entity.
- Columns B through E define the path of the object.
  - Rows 3, 5, 6, and 7 contain existing Process objects that require updating. With the exception of Row 5 (an existing object that will be disassociated), Columns C, D, and E can remain blank for existing objects.
  - Rows 2 and 4 contain information for the creation of new Process objects. Path and parent object information is provided in Columns C, D, and E for each new object to be created.
- Columns F through Z represent object-specific fields.

	A	B	C	D	E	F	G
1	Remove Association	Folder Path	Parent Path	Parent Object Types	Parent Objects	Name	Description
2		/North America/United States	/North America/United States	SOXBusEntity	United States	Proc-U02	Payroll
3		/North America/United States/Boston				Proc-B01	Payroll
4		/North America/United States/Boston	/North America/United States/Boston	SOXBusEntity	Boston	Proc-B02	Payroll
5	Y	/North America/United States/Boston	/North America/United States/Boston	SOXBusEntity	Boston	Proc-B03	Funds Transfer
6		/North America/United States/Boston				Proc-B04	Payroll
7		/North America/United States/Cleveland				Proc-C01	Payroll

Figure 70. Sample Processes Worksheet

## Sample Risks worksheet

The sample Risks worksheet in the Sample Risks Worksheet shows the following:

- Column A, row 4 contains an existing Risk object (Risk-N01) under the North America entity. The Y in this column will result in Risk-N01 being deleted from the repository.
- Columns B through E define the path of the object. Notice the following:
  - Rows 2 - 6 contain existing Risk objects that require updating (notice that Columns C, D and E can remain blank for existing objects).
  - Row 7 contains information for the creation of a new Risk object (notice that path and parent object information is provided in Columns C, D and E).
- Columns F through Z represent object-specific fields.

	A	B	C	D	E	F	
1	Delete	Folder Path	Parent Path	Parent Object Types	Parent Objects	Name	Description
2		/North America/United States/Boston				Risk-B01	Payroll
3		/North America/United States/Cleveland				Risk-C01	Payroll
4	Y	/North America				Risk-N01	Payroll
5		/North America/United States				Risk-U01	Payroll
6		/North America/United States/Boston				Risk-B02	Payroll
7		/North America/United States/Boston	/North America/United States	SOXControlObjective	CO-B01	Risk-B03	Payroll

Figure 71. Sample Risks Worksheet

## Sample self-contained object worksheet

If you are adding self-contained objects, such as Processes in a Process-based security model, these objects must reside under their own folder. This folder must match the object name.

**Important:** You must specify the container folder for a self-contained object.

Table 235 on page 778 shows how to specify folder and parent paths for Process objects in a Process-based security model. In this example, the Process folder is named PR-200 and is appended after the Business Entity Boston folder.

Notice that the Folder Path column contains the name of the PR-200 Process folder.

	A	B	C	D	E	F	G
1	Delete	Folder Path	Parent Path	Parent Object Types	Parent Objects	Name	Description
2		/North America/United States/Boston/PR-200	/North America/United States/Boston	SOXBusEntity	Boston	PR-200	Payroll
3							

Figure 72. Sample Worksheet for Process Objects (Process Security Model)

Figure 73 on page 783 shows how to specify folder and parent paths for child Risk objects in a Process-based security model. Similarly, in this example, the Process folder is named PR-200

Notice that both the Folder Path and Parent Path columns contain the name of the Process folder, PR-200.

A	B	C	D	E	F	G
1 Delete	Folder Path	Parent Path	Parent Object Types	Parent Objects	Name	Description
2	/North America/United States/Boston/PR-200	/North America/United States/Boston/PR-200	SOXProcess	PR-200	Risk-200	Pay

Figure 73. Sample Worksheet for Risk Objects (Process Security Model)

## Sample Business Entity worksheet for creating a new business entity structure

The sample business structure in Sample Business Entity Structure shows three levels of business entities.

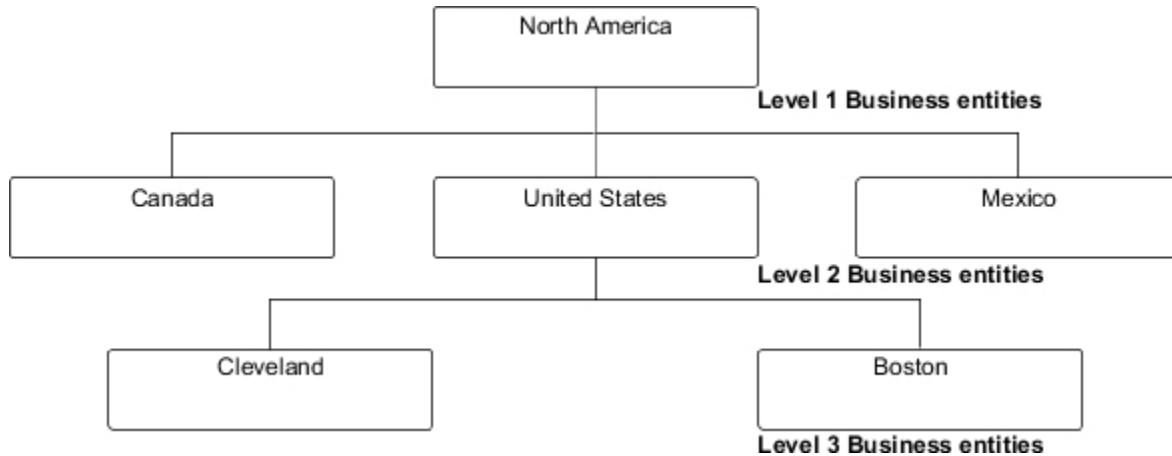


Figure 74. Sample Business Entity Structure

To create new Business Entity objects that map to the structure in Figure 74 on page 783, you would create a Business Entities object worksheet in Microsoft Excel similar to the one shown in Figure 75 on page 783.

The sample Business Entities worksheet in Figure 75 on page 783 creates new entities and shows the following:

- Column A is an optional field that can be used to delete existing objects. Since all the objects in this worksheet are new, none are marked for deletion (by default, the value is N for no - do not delete).
- Columns B through E define the path of the new object. Notice that Row 2 contains the top-level Business Entity (North America), so the Parent Path and Parent Objects columns are blank.
- Columns F through Z represent object-specific fields.

A	B	C	D	E	F	G	H
1 Delete	Folder Path	Parent Path	Parent Object Types	Parent Objects	Name	Description	Entity Type
2	/North America		SOXBusEntity		North America	Global Headquarters	Headquarters
3	/North America/United States	/North America	SOXBusEntity	North America	United States	North America - US	Region
4	/North America/United States/Cleveland	/North America/United States	SOXBusEntity	United States	Cleveland	Central Regional Sales	Region
5	/North America/United States/Boston	/North America/United States	SOXBusEntity	United States	Boston	Sales	Region
6	/North America/Canada	/North America	SOXBusEntity	North America	Canada	North America - Sales Office	
7	/North America/Mexico	/North America	SOXBusEntity	North America	Mexico	North America - Mexico	Sales Office

Figure 75. Sample Business Entity Worksheet

## Using the FastMap Definition worksheet

You can include a Definition worksheet in a workbook to configure FastMap behavior.

When you export data from IBM OpenPages with Watson, by default the Definition worksheet is not hidden from users in the workbook, and does not have column headings.

By default, the following parameter values are set:

Table 239. FastMap Definition worksheet default parameters

Parameter	Value
ignoreReadOnlyWarnings	TRUE
locale	en_US
profileName	Default
exportDate	The date and time the data was exported. Example: 24-Jul-2009 10:12:52 AM

Parameters that are listed in a Definition worksheet will override settings from other sources, such as JSP report parameters.

For more information, see [“FastMap parameters for importing and exporting data” on page 786](#).

## Unhiding a FastMap Definition worksheet

If you do not see the Definition worksheet in a FastMap template workbook, and you want to change or add parameters to it, then you must unhide the worksheet.

By default, the Definition worksheet is not hidden.

### Procedure

1. In Microsoft Excel, select the workbook with the hidden Definition worksheet.
2. From the toolbar select **Format | Sheet | Unhide**.
3. In the **Unhide** box, select **Definition** and click **OK**.
4. Save the file.

## FastMap parameters

You can use FastMap parameters to customize how data is imported (uploaded) to and exported from the IBM OpenPages with Watson application.

To set FastMap parameters, list parameter names on the Definition worksheet of a FastMap template.

## FastMap export templates

An export template is used to format object data exported into a Microsoft Excel workbook.

By configuring parameters on the Definition worksheet of an export template, you can control the behavior of the export or its subsequent import.

Unless another template is specified, the IBM OpenPages with Watson application uses DefaultTemplate.xlsx as the default export template.

## Modifying parameters in the default FastMap export template

To add or modify parameters in the default export template, use the following steps.

### Before you begin

To perform this procedure, you must have the **OpenPages Platform 3** profile associated with your username.

## About this task

By default, the Definition worksheet in the DefaultTemplate.xlsx file has only the ignoreReadOnlyWarnings parameter set to TRUE. You can modify the template to include other parameters.

## Procedure

1. Click  > **System Configuration** > **System Files**.
2. Expand the **Templates** > **FastMap** > **FLV** folder and locate the DefaultTemplate.xlsx file.
3. Modify the DefaultTemplate.xlsx file, save it, and check it in. For more information about editing Microsoft Office files directly from OpenPages, see *Adding and working with files (attachments) on objects in the IBM OpenPages with Watson User Guide*.  
Available parameters are listed in [Table 241 on page 786](#) in *FastMap Definition worksheet import-only parameters*.

## Specifying a FastMap export template

The IBM OpenPages with Watson application supports multiple export templates.

You can specify export templates based on one or more of the following criteria:

- ContentType
- Locale
- Profile

Use the following rules when specifying criteria for an export template:

1. Criteria are specified in the name of the export template.
2. Each criterion is separated in the template name by a hyphen.
3. The criteria must be specified in this order: ContentType-Locale-Profile

The system selects templates based on the following precedence: ContentType -> Locale -> Profile.

For example, SOXRisk.xlsx will be selected before DefaultTemplate-en\_US-FCM Module.xlsx, and SOXRisk-All-FCM Module.xlsx will be selected before SOXRisk.xlsx

**Note:** If no match is found, the DefaultTemplate.xlsx export template is used.

The syntax for the export template name is:

```
<ContentType>-<Locale>-<Profile>.xlsx
```

Where:

<ContentType> is the system name of an object type (such as, SOXRisk), not the localized name. To specify all object types, use DefaultTemplate for the <ContentType>.

<Locale> is the language and locale code (for example, en\_US). To specify all locales, use All for the <Locale>.

<Profile> is the name of a profile in the OpenPages with Watson application.

For purposes of illustration, the examples listed in [Table 240 on page 785](#) for specifying criteria in export templates use the Risk object type (SOXRisk) in the U.S. English locale (en\_US) for users assigned the FCM Module profile.

*Table 240. Example syntax for specifying criteria*

If you want to specify...	Example syntax...
a specific object type for a specific locale and profile	SOXRisk-en_US-FCM Module.xlsx

*Table 240. Example syntax for specifying criteria (continued)*

If you want to specify...	Example syntax...
all object types (use DefaultTemplate) for a specific locale and profile	DefaultTemplate-en_US-FCM Module.xlsx
all locales (use All) for a specific object type and profile	SOXRisk-All-FCM Module.xlsx
all locales and all profiles for a specific object type	SOXRisk.xlsx
all profiles for a specific object type and locale	SOXRisk-en_US.xlsx
a specific profile for all object types and locales	DefaultTemplate-All-FCM Module.xlsx

**Note:** Subsets must honor ordering. For example, the following template names would be invalid:

FCM Module.xlsx - this is an invalid template name because the profile name must be the third criterion in the list (not the first).

en\_US-FCM Module.xlsx - this is an invalid template name because the locale must be the second (not the first) and profile name must be the third (not the second) criterion in the list.

## FastMap parameters for importing and exporting data

The following table lists the various FastMap parameters that you can use on a Definition worksheet to configure FastMap behavior.

*Table 241. FastMap Definition worksheet import-only parameters*

Import-only Parameter Name	Default Value	Description
allowOrphans	FALSE	<p>Determines if objects will be created when no parent object is specified.</p> <p>If the value is set to:</p> <ul style="list-style-type: none"> <li>• TRUE - creates an object if no parent is specified</li> <li>• FALSE - create an object only if a parent is specified</li> </ul>
disableConflictDetection	FALSE	<p>Determines if objects have been modified in the system since you last exported data into the worksheet.</p> <p>When a worksheet is exported from IBM OpenPages with Watson, it is marked with the time of the export. When data is imported back into the system, any objects that have been updated after this time will result in a validation message alerting the user and will not be updated.</p> <p>If the value is set to:</p> <ul style="list-style-type: none"> <li>• TRUE - no validation warnings will be displayed and the worksheet values will override any recent changes in the system.</li> <li>• FALSE - a validation warning will be displayed and the object will not be updated.</li> </ul>

Table 241. FastMap Definition worksheet import-only parameters (continued)

Import-only Parameter Name	Default Value	Description
fullLoad	FALSE	<p>Used when the data in your worksheet is a complete representation of what should be in the OpenPages with Watson repository.</p> <p>If used in conjunction with the parentResource parameter, only objects under that resource will be affected.</p> <p>Object types that are not being uploaded will not be deleted in the system.</p> <p>If the value is set to:</p> <ul style="list-style-type: none"> <li>• TRUE - any objects that are not in the set being uploaded will be deleted.</li> <li>• FALSE - any objects that are not in the set being uploaded will be retained.</li> </ul>
ignoreColumns	null	<p>Use if you want to include an additional column on a worksheet for information, and you want that column to be ignored by FastMap during validation.</p> <p>For example, "column1;column2"</p>
ignoreEmptyFields	TRUE	<p>Determines whether empty fields are blanked out during updates.</p> <p>If the value is set to:</p> <ul style="list-style-type: none"> <li>• TRUE - empty fields are ignored and not modified during an update.</li> </ul> <p>To explicitly clear a field, set its value to *blank*.</p> <p><b>Note:</b> If you're using a locale other than English, you can use *blank* or the value that is specified in the application text com.fm.label.blank.field</p> <ul style="list-style-type: none"> <li>• FALSE - empty fields will be blanked out during an update.</li> </ul>
ignoreHiddenEnumWarnings	TRUE	<p>Determines whether warning messages are displayed when values are submitted for hidden enumerated strings on a field in the OpenPages with Watson application.</p> <p>If the value is set to:</p> <ul style="list-style-type: none"> <li>• TRUE - no warning is displayed for hidden enumerated string values, whether changed or not.</li> <li>• FALSE - a warning is displayed for hidden enumerated string values, whether changed or not.</li> </ul> <p>Hidden enumerated string values that have been changed on objects will be updated during the import process regardless of the value of this setting.</p>

Table 241. FastMap Definition worksheet import-only parameters (continued)

Import-only Parameter Name	Default Value	Description
ignoreReadOnlyWarnings	FALSE	<p>If data is being uploaded into fields that are defined as read-only, OpenPages with Watson will display a warning message indicating that these values will be ignored.</p> <p>Use this setting to hide or display warning messages for read-only fields. Regardless of the whether warning messages are displayed, the data will not be uploaded.</p> <p>If the value is set to:</p> <ul style="list-style-type: none"> <li>• TRUE - warning messages are hidden.</li> </ul> <p><b>Note:</b> This value is set to TRUE in the default template when you export data from OpenPages with Watson.</p> <ul style="list-style-type: none"> <li>• FALSE - warning messages are displayed.</li> </ul>
ignoreSheets	null	<p>Use if you want to include an additional worksheet for information, and you want that worksheet to be ignored by FastMap during validation.</p> <p>For example, "sheet1;sheet2".</p>
parentResource	null	<p>When set to the full path of an object, this parameter is used for all parent associations. All other parent information in the worksheet will be ignored.</p>
shouldDefaultNotRequiredFields	TRUE	<p>Determines whether default values will be used for all non-required fields that are missing values in a worksheet.</p> <p>If the value is set to:</p> <ul style="list-style-type: none"> <li>• TRUE - default values will be used for non-required fields that are missing values in a worksheet.</li> <li>• FALSE - no default values will be used for non-required fields that are missing values in a worksheet.</li> </ul>
shouldDefaultRequiredFields	TRUE	<p>Determines whether default values will be used for all required fields that are missing values in a worksheet.</p> <p>If the value is set to:</p> <ul style="list-style-type: none"> <li>• TRUE - default values will be used for required fields that are missing values in the worksheet.</li> <li>• FALSE - required fields that are missing values in the worksheet will display validation errors.</li> </ul>

Table 241. FastMap Definition worksheet import-only parameters (continued)

Import-only Parameter Name	Default Value	Description
shouldValidateBESelector	TRUE	<p>Determines whether Business Entity Selector display fields are validated during import.</p> <p>If the value is set to:</p> <ul style="list-style-type: none"> <li>• TRUE - a warning will be displayed for any business entity that does not exist.</li> <li>• FALSE - no validation will be done on Business Entity Selector fields.</li> </ul> <p>Warnings are displayed for incorrect or invalid values. For example, a warning is shown for a wrong value, such as a typographical error. In this case, you might not want to load the data.</p> <p>Warnings are also displayed in cases where a value changed making it currently invalid. For example, you exported data from OpenPages and then reimported the data later by using FastMap. The data can be flagged as invalid because a field value moved, was renamed, or been deleted. In this case, you might want to load the data because it was accurate in its original state.</p>
shouldValidateRequiredFields	TRUE	<p>Determines whether fields configured as required in the Profile are validated during import.</p> <p>If the value is set to:</p> <ul style="list-style-type: none"> <li>• TRUE - required fields will be validated.</li> <li>• FALSE - required fields will not be validated.</li> </ul>
suppressWarnings	FALSE	<p>Determines whether warning conditions will be displayed.</p> <p>If the value is set to:</p> <ul style="list-style-type: none"> <li>• TRUE - warning conditions will not be displayed.</li> <li>• FALSE - warning conditions will be displayed.</li> </ul>
useFirstInstance	TRUE	<p>Determines whether to use and validate only the first instance of an object when multiple instances of the same object are in a worksheet.</p> <p>If the value is set to:</p> <ul style="list-style-type: none"> <li>• TRUE - only the first instance of the object will be used to update the object.</li> <li>• FALSE - only the last occurrence of the object will be used to update the object.</li> </ul>

*Table 242. FastMap Definition worksheet import and export parameters*

<b>Import and Export Parameter Name</b>	<b>Default Value</b>	<b>Description</b>
exportDate	null	<p>When exporting data from OpenPages with Watson, this parameter is set, by default, to the current date and time.</p> <p>During the import validation process, each object is checked against the export timestamp. If changes to an object are more recent than the date and time of the export timestamp, a conflict exception warning message will be displayed during validation. The message alerts the user that they may be overwriting more recent changes made to an object.</p> <p>To disable this behavior you can set the disableConflictDetection parameter to TRUE.</p>
headerRow	1	The row in the worksheet that stores the column headers.
locale	null	<p>If a locale value is:</p> <ul style="list-style-type: none"> <li>Not specified - the locale of the user will be used during validation.</li> <li>Specified - the locale value that is set (such as, en_US, ja_JP, de_DE) will override the user's locale during validation.</li> </ul>
multiSelectDelim	\r\n	<p>Delimiter for multi-select enumeration lists.</p> <p>The default for Microsoft Excel is carriage return line feed that can be entered in Excel by using the Alt+Enter key sequence.</p>
profileName	null	The name of the profile to validate against. If null, the profile of the currently logged-on user is used.
useSystemNames	FALSE	<p>By setting this parameter to TRUE FastMap will use the system names of the fields, not the localized labels, for column headers. System names are in the format [FIELD GROUP].[FIELD NAME]. For example, OPSSEnt.Domain. When exporting, the labels will also be included on another row as a convenience.</p> <p>The useSystemNames parameter has no effect on enumerated values or their localized labels.</p>

*Table 243. FastMap Definition worksheet export-only parameters*

<b>Export-only Parameter Name</b>	<b>Default Value</b>	<b>Description</b>
exportActorDisplayName	FALSE	If the value is set to TRUE, creates an additional <field_name>.Display Name column for actor fields. For example, an Executive Owner.Display Name column can be created for the Executive Owner actor field.

Table 243. FastMap Definition worksheet export-only parameters (continued)

Export-only Parameter Name	Default Value	Description
exportBaseAmount	TRUE	<p>When exporting currency field data from OpenPages with Watson, this parameter determines whether to include a column for the Base Amount.</p> <p>If the value is set to:</p> <ul style="list-style-type: none"> <li>• TRUE - the Base Amount field is included.</li> <li>• FALSE - the Base Amount field is excluded.</li> </ul>
exportBaseCode	TRUE	<p>When exporting currency field data from OpenPages with Watson, this parameter determines whether to include a column for the Base Code.</p> <p>If the value is set to:</p> <ul style="list-style-type: none"> <li>• TRUE - the Base Code field is included.</li> <li>• FALSE - the Base Code field is excluded.</li> </ul>
exportComputedFields	TRUE	<p>Determines if computed fields will be evaluated and their values exported with other fields.</p> <p>If the value is set to:</p> <ul style="list-style-type: none"> <li>• TRUE - computed fields will be evaluated and their values exported with other fields.</li> <li>• FALSE - computed fields will be ignored during export.</li> </ul>
exportExchangeRate	TRUE	<p>When exporting currency field data from OpenPages with Watson, this parameter determines whether to include a column for the Exchange Rate.</p> <p>If the value is set to TRUE, the Exchange Rate field is included.</p> <p>If the value is set to FALSE, the Exchange Rate field is excluded.</p>

Table 243. FastMap Definition worksheet export-only parameters (continued)

Export-only Parameter Name	Default Value	Description
exportParentInfo	PRIMARY	<p>This optional parameter specifies whether the object parent information is included or excluded from the export. You can specify the value of TRUE, FALSE, or PRIMARY for this parameter.</p> <p>When this parameter is set to TRUE, the parent information is included in the export. The <b>Parent Path</b>, <b>Parent Object Types</b>, and <b>Parent Objects</b> columns are filled out in the target object worksheet. If an object in the worksheet has multiple parents, one row with the unique parent\folder information is included for each parent, and the object field information is repeated in each row for that object. The resulting FastMap format worksheet can be used to load the objects and their associations to another system that does not contain these object and association instances, but has the same configured object types and associations, fields, and profiles. The data on the loaded target system will be the same as on the source system from which the content was exported. However, the export performance is slower when this parameter is set to TRUE.</p> <p>When this parameter is set to FALSE, data for <b>Parent Path</b>, <b>Parent Object Types</b>, and <b>Parent Objects</b> columns is not exported.</p> <p>When this parameter is set to PRIMARY, is not specified, or has an invalid value on the Definitions worksheet, the <b>Parent Path</b>, <b>Parent Object Types</b>, and <b>Parent Objects</b> columns in the target worksheet are filled out only for the primary parent. If an object has multiple parents, the non-primary parents are not exported.</p>

Table 243. FastMap Definition worksheet export-only parameters (continued)

Export-only Parameter Name	Default Value	Description
highlightDuplicates	TRUE	<p>For objects with multiple parents, this parameter is used to display the duplicated parent information by using the light-gray, italicized font to de-emphasize this information. The values are TRUE or FALSE. This parameter is dependent on the useFirstInstance import parameter.</p> <p>When this parameter is set to TRUE, and the useFirstInstance parameter is also set to TRUE, the first instance of the object parent information is displayed using the standard font style, and the subsequent, duplicated information is de-emphasized. If useFirstInstance is set to FALSE, the last instance of the object parent information is displayed using the standard style, and the previous, duplicate information is styled based on the highlightDuplicates parameter. Styles that are inherited from the export template are maintained.</p> <p>When this parameter is set to FALSE, the style of the information for objects with multiple parents is unchanged. The files exported with the highlightDuplicates and useFirstInstance parameters can be imported through FastMap without changes if the user does not make any changes to the data in the worksheet. If there are multiple records for an object in the worksheet because multiple parents are exported, the only object from which updates are recognized by FastMap is based on the useFirstInstance parameter (default value TRUE).</p>
includeHTMLTags	FALSE	<p>Determines if HTML tags are exported for Rich Text Field formatted data.</p> <p>Rich Text Field data that is exported without HTML tags can be more easily read in the spreadsheet. However, if this field is updated and then imported into FastMap, the field will be imported as plain text as it has lost its formatting.</p> <p>If the value is set to:</p> <ul style="list-style-type: none"> <li>• TRUE - HTML tags are exported with the data.</li> <li>• FALSE - HTML tags are not exported with the data.</li> </ul>

## Configuring a lookup key for FastMap

If you are importing data from an external system, you can use a field other than the Name field to identify objects. Use the settings described in Table 244 on page 794 to configure a lookup key for FastMap and set the scope of the lookup. This technique is most useful when you want to update data with existing records from an external system and synchronize it with records in OpenPages with Watson.

**Note:** You can only use object fields with the data type of Simple String, Integer, or Enumerated String as lookup keys.

For example, you want to import risk data from an external system into the OpenPages with Watson repository. Data from the external system has a unique ID field that you want to keep and use as a lookup key within OpenPages with Watson.

You would create a custom field group and field definition within OpenPages with Watson for the Risk object type (SOXRisk) for the ID field in the external system, for example, ExternalSys\_A.Risk\_ID.

You would then use the custom field group and field definition, ExternalSys\_A.Risk\_ID, to configure the Key setting for FastMap. After this setting is configured, you would add a column to your FastMap template for the Risk\_ID field and populate it with values from the external system's ID field. When you import data from the external system, FastMap would then match records based on this field.

You can also scope the update of Risk data under a specific parent object. By setting the Scoped value to true, FastMap would only update objects under the parent that is specified in the worksheet.

## Procedure

1. For each object type for which you want a lookup key, configure a field group and field definition (see Chapter 10, “Fields and field groups,” on page 153).
2. Configure the key fields settings for FastMap as follows:
  - a) Access the **Settings** page (see Chapter 20, “Viewing the Configuration and Settings page,” on page 473).
  - b) Expand the **Applications > GRCM > FastMap > Key Fields** folder hierarchy.
  - c) Navigate to the object type folder that you want and then expand the folder to see its settings.
  - d) For each object type for which you want to define a lookup key, modify the following settings as needed:

*Table 244. Lookup key settings*

Setting Name	Description
Key	<p>Used by FastMap to lookup objects when the name is not provided in a worksheet. Generally used in scenarios when objects are auto-named.</p> <p>The format is</p> <pre>field_group.field_name</pre> <p>Where:</p> <p>field_group is the name of the field group.</p> <p>field_name is the name of the object field.</p> <p>Example</p> <pre>ExternalSys_A.R_ID</pre> <p>If you have multiple fields, use a comma to delimit the fields. For example:</p> <pre>field_group.field_name,field_group.field_name</pre>
Scoped	<p>Used by FastMap to determine whether to lookup the value in the <b>Key</b> setting only under the parent objects or across all objects.</p> <p>If the value is set to:</p> <ul style="list-style-type: none"><li>• <b>true</b> - the lookup is scoped only under parent objects. This is the default.</li><li>• <b>false</b> - the lookup is not scoped and is across all objects.</li></ul>

- e) Click a setting.
- f) In the **Value** field, type a value.
- g) When finished, click **Done**.

The effect of the change is immediate.

3. In the FastMap template:

- a) For each field name that matches a <field name> value in the Key setting (from Step 2d), add a corresponding column to the template.
- b) Populate each corresponding column with values from your external system.
- c) When finished, import the template into FastMap.

## Modifying export settings to optimize FastMap performance

---

Data is typically exported for an object type, modified, and imported back into FastMap.

To optimize and control the export of data, you can configure the following settings:

- **Maximum Export Size** - for details, see [“Maximum number of objects to export to Microsoft Excel from Grid Views” on page 495](#).
- Concurrent Exports - for details, see [“Maximum concurrent export requests” on page 497](#).

## Limiting the rows for import to optimize FastMap performance

---

You can use the **Maximum Workbook Rows** setting to limit the number of rows that can be imported from a FastMap template.

By default, the value is set to 20000 rows (recommended maximum).

**Note:** Setting the number of rows for import above the recommended maximum of 20000 rows may result in slower performance and longer processing time. However, if you choose to set this value higher, then the processing timeout value in the **Transaction timeout** setting should also be increased (see [“Setting a transaction timeout to optimize FastMap performance” on page 795](#) for details).

If the number of rows being imported exceeds the set value, then a validation error will be displayed stating that the workbook exceeds the allowable size.

For example, if the Maximum Workbook Rows setting has a value of 2500 and a user wants to import data into IBM OpenPages with Watson for Risk and Control objects, the workbook for the FastMap template contains:

- a worksheet for Risk objects with 1,000 rows of data
- a worksheet for Control objects with 2,000 rows of data
- a Definition worksheet with 5 rows of data

The total number of rows with data in the workbook is 3,005. Since the workbook exceeds the allowable size, a validation error will be displayed to the user.

### Procedure

1. Access the **Settings** page (see [Chapter 20, “Viewing the Configuration and Settings page,” on page 473](#)).
2. Expand the **Applications > GRCM > FastMap** folder hierarchy.
3. Click the **Maximum Workbook Rows** setting.
4. In the **Value** field, type a number greater than zero (for example, 2500).
5. Click **Done**.

## Setting a transaction timeout to optimize FastMap performance

---

If you set the value in the **Maximum Workbook Rows** setting above the recommended maximum of 20000 rows, you can use the **Transaction timeout** setting to increase the maximum time a process can run before it times out and stops.

By default, the value is set to 7200 seconds (2 hours).

### Procedure

1. Access the **Settings** page (see [Chapter 20, “Viewing the Configuration and Settings page,” on page 473](#)).
2. Expand the **Applications > GRCM > FastMap** folder hierarchy.
3. Click the **Transaction timeout** setting.
4. In the **Value** field, type a number greater than 7200 (the value represents seconds).
5. Click **Done**.

## Adding a processing delay to optimize FastMap performance

---

To reduce the processing impact of FastMap data imports on a system, you can use the **Process Delay** setting to set a delay in milliseconds between each record. If a value is set, the time to process the imported data will be extended.

By default, the value is set to 0 (zero).

### Procedure

1. Access the **Settings** page (see [Chapter 20, “Viewing the Configuration and Settings page,” on page 473](#)).
2. Expand the **Applications > GRCM > FastMap** folder hierarchy.
3. Click the **Process Delay** setting.
4. In the **Value** field, type a number greater than zero.
5. Click **Done**.

## Securing FastMap import templates stored on the server

---

You can use the **Encrypt FastMap Files** setting to configure security on FastMap import templates that are stored on the server.

By default, the value is set to `true`, which encrypts FastMap import templates stored on the server.

**Note:** Before you change the value of the **Encrypt FastMap Files** setting, check the status of FastMap import jobs to verify that no FastMap imports are pending processing. For more information about checking import status, see [“Accessing FastMap to import data and view status” on page 770](#).

If you change the value of this setting while FastMap processes are pending, the import will fail even if the templates have passed data validation.

### Procedure

1. Access the **Settings** page (see [Chapter 20, “Viewing the Configuration and Settings page,” on page 473](#)).
2. Expand the **Applications > GRCM > FastMap** folder hierarchy.
3. Click the **Encrypt FastMap Files** setting.
4. In the **Value** field, type one of the following values.

If the value is set to:

- **true** - FastMap import templates are encrypted when stored on the server. This is the default.
- **false** - FastMap import templates are not encrypted when stored on the server.

5. Click **Done**.

## Cleaning up FastMap import templates stored on the server

---

You can use the **Delete After Days** setting to configure the maximum number of days that a FastMap import template can remain on the server before it is automatically deleted.

FastMap import templates that will automatically be deleted from the server include templates that have:

- Finished processing - either successfully or with errors/warnings
- Exceed the maximum number of days specified in the **Delete After Days** setting. By default, this value is set to delete FastMap import templates after 1 day.

**Note:** A FastMap import template that is older than the default value of 1 day will be automatically deleted regardless of whether or not the template has completed processing. Use a higher value for this setting if you upload large amounts of data using FastMap import templates.

### Procedure

1. Access the **Settings** page (see [Chapter 20, “Viewing the Configuration and Settings page,” on page 473](#)).
2. Expand the **Applications > GRCM > FastMap** folder hierarchy.
3. Click the **Delete After Days** setting.
4. In the **Value** field, type a number greater than zero. By default, this value is set to 1.
5. Click **Done**.

## Using FastMap with questionnaire template and assessment objects

---

You can use FastMap to import and export questionnaire template objects and the content in sections, subsections, and questions. You can also use it to import and export the standard fields for questionnaire assessment instances. However, you cannot use it import or export content, for example, question answers, comments, and attachments, on questionnaire assessment instances.

### About this task

You can import and export content for the following objects:

- Questionnaire templates
- Section template
- Subsection template
- Question template
- Questionnaire assessments (standard fields only)

The **Enumerated Answers** field in the questionnaire template stores single and multiple choice answers in JSON format. You cannot add this field to the object profile views. However, you can import and export it.

Every question in a questionnaire template has an internal identifier that is stored in the **ReportID** field. You can import a questionnaire template and leave the **ReportID** fields empty. You should then launch a program that uses the questionnaire template so that the system can assign **ReportID** values. The **ReportID** values are required for questionnaire templates and assessments to work correctly. In particular, when you copy answers from one questionnaire assessment to another, the system requires the **ReportID** values to identify questions and their answers. For more information, see *Launching a program and copying answers* in the *IBM OpenPages with Watson User Guide*.

## Example

A question has three possible answers: Yes, No, and N/A, without descriptions and scores:

```
[{"value": "Yes"}, {"value": "No"}, {"value": "NA"}]
```

A question has two answers, Yes and No, where both answers have descriptions and scores:

```
[{"value": "Yes", "score": 20, "description": "description for Yes"}, {"value": "No", "score": 30, "description": "description for Yes"}]
```

A question has three answers, Yes, No, and N/A, where Yes requires a comment, No requires an attachment, and N/A requires both:

```
[{"value": "Yes", "score": 20, "requires": ["comment"]}, {"value": "No", "score": 30, "requires": ["attachment"]}, {"value": "NA", "score": 40, "requires": ["comment", "attachment"]}]
```

## Exporting and importing tags with FastMap

---

A list of tags for each object is exported and imported with FastMap when tagging is enabled in OpenPages.

For more information about enabling and disabling tagging, see [“Creating tags” on page 237](#).

The following rules apply to importing and exporting tags with FastMap:

- On import, if a tag is included in the import but it doesn't already exist in the system, a validation warning is reported and the tag is not imported.
- Tagging is disabled in OpenPages.
  - On import, if the spreadsheet includes the Tags column but tagging is disabled in OpenPages, a validation warning is reported.
  - On export, if tagging is disabled, tags are not exported.
- Tags that are imported do not match tags on the object in OpenPages.
  - If FastMap import is updating an existing object that has a tag that is not included in the spreadsheet, the tag is removed from the object. For example, if BE1 has tags Tag1 and Tag 2, and the FastMap spreadsheet includes BE1 with tag Tag 2, then Tag1 is removed from BE1.
  - If FastMap import is updating an existing object with a tag and the tag exists in OpenPages, then the tag is applied to the object. For example, if BE1 has tag Tag 2, and the FastMap spreadsheet includes BE1 with tags Tag 2 and Tag 3, then Tag 3 is added to BE1 on import if the tag exists already in OpenPages.
- If the FastMap spreadsheet contains tags that would result in a system error, a validation error is reported. For example, a validation error is reported if the import would result in more than 25 tags on an object.

# Chapter 29. Configuring and generating the reporting framework

You can configure IBM OpenPages with Watson to use IBM Cognos Analytics for your organization's reporting requirements.

## The reporting framework

The reporting framework consists of Cognos framework models that are configured and generated in OpenPages. They support relational data used for creating reports in IBM Cognos Analytics.

When you generate the reporting framework, packages for selected framework models are published to the Cognos server. Using the query subjects and query items in these namespaces, report authors can create reports from within IBM OpenPages with Watson.

For more information, see the *IBM OpenPages with Watson Report Author's Guide*.

**Note:** "V6" refers to the latest framework version, not to any specific OpenPages release number.

## Framework models

Framework models are based on the OpenPages object model and define subsets of objects and relationships necessary for your reporting requirements.

Framework models include the following components:

- Metadata
- Labels
- Custom query subjects

The reporting framework contains a set of pre-defined framework models, which are used for the pre-defined reports that are supplied with OpenPages. In addition to the pre-defined framework models, you can create your own framework models. The ability to use multiple framework models allows you to target a framework model to specific solutions, user roles, or object profiles.

There are two types of framework models that you can create:

- Standard
- Basic

Both types support profile filtering and allow you to define the package name.

### Standard framework models

Standard framework models are intended for advanced report writers with extensive knowledge of IBM Cognos Analytics. Use this type of model for reports that require the more complex functionality that Cognos offers.

Standard framework models have the following characteristics:

- Nest a relationship subnamespace.
- Use the following namespace hierarchy:
  - **[package label] > [namespace] > [namespace]\_REL**
- Use extensive foldering for query subjects and data items.
- Contain query subjects for ancillary objects such as Enumerations and Relationships.

- Use complex field representations, for example, currencies have multiple data items for local and base amount.
- Represent recursive objects as multiple query subjects using recursive object levels.
- Provide secondary compliance objects, such as Files or Issues, as stand-alone objects. Relationships to them must be built in reports.

## **Basic framework models**

Basic models are intended for end users who do not have extensive knowledge of IBM Cognos Analytics. Use this type of model for more simple reports that you want to allow your end users to create as they require.

Basic framework models have the following characteristics:

- Use the following namespace hierarchy: **[package label] > [namespace]**

Query subjects are created in the root namespace. The [namespace]\_REL sub-namespace is not created.

- Do not create ancillary query subjects for Enumerations, relationships, and so on.
- Generate recursive objects, for example, Business Entity, SubMandate, and SubProcess, as single query subjects.
- Generate recursive object levels only for Business Entity objects.
- Remove system-level data items, for example, IS\_PRIMARY, LATEST\_VERSION, and so on.
- Use simplified field representations, for example, single data items for Currencies and Enumerations as Local Amount and Localized Value, respectively.

## **More information**

To configure framework models, see the following topics:

- [“Configuring settings that apply to all framework models” on page 806](#)
- [“Configuring framework models ” on page 810](#)
- [“Configure reporting framework namespaces” on page 812](#)

## **Namespaces**

A namespace uniquely identifies a collection of query subjects, their relationships, and other objects (such as calculations) that you can use for authoring reports.

The framework generator uses the definition of a namespace (which is defined in the IBM OpenPages with Watson user interface) to create a corresponding namespace in the framework model.

The namespaces in the pre-defined framework models are used by the pre-defined reports that are supplied with OpenPages. If you make changes to the namespaces, it can affect the functionality of the reports and might cause them to fail to run. You can add your own namespaces to the pre-defined framework models to uniquely identify a collection of query subjects and other objects (such as calculations) for satisfying your reporting requirements

If you define your own standard and basic framework models, you must define namespaces for them.

### **Standard framework models**

When you generate the reporting framework, the packages for the standard framework models are published to the Cognos server with a relationship subnamespace:

- [namespace]\_REL – this relational namespace enables report authors to report on objects based upon their defined relationships. This type of model is often used in list reports that use mixed data (numeric, data, and string).

## Basic models

When you generate the reporting framework, the packages for basic framework models are published to the Cognos server. Query subjects are created in the root namespace. Sub-namespaces are not created.

For more information, see [“Configure reporting framework namespaces” on page 812](#).

For more information about namespaces and the framework model, see the *IBM OpenPages with Watson Report Author’s Guide*.

## Triangle object relationships

A triangle object relationship exists when one child has two parents that are related to each other.

To enhance report authoring capability, use the **Supported Triangle Relationships** setting to configure object types with triangle relationships in the reporting framework relational data model.

Within the triangle, the “top” (parent 1) and “bottom” (child) object types are non-recursive. The “middle” (parent 2) object type is recursive (such as Sub-Process). For more information about recursive objects, see [“Recursive object levels” on page 802](#).

A triangle relationship that includes two recursive object types is not supported.

For example, a report author has a requirement to create a Risk report that allows business users to assess risks associated with various processes and sub-processes within the company.

To provide the report author with easier reporting capability in the framework model, you could configure a triangle relationship between the non-recursive child Risk object and its two related parents: a non-recursive parent Process object and a recursive parent Sub-Process object type, as shown in [Figure 76 on page 801](#).

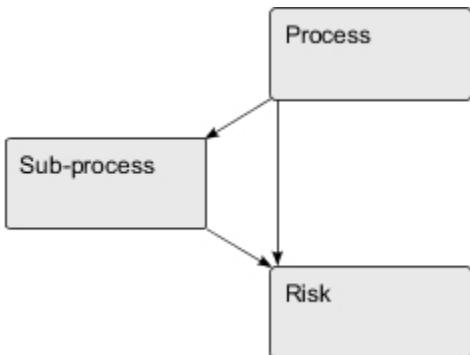


Figure 76. Triangle relationship between objects

The path between the objects that forms a triangle relationship must be reflected in a namespace within the reporting framework. For example, a namespace might have the following object type hierarchy configured for Business Entity, Process, Sub-Process, and Risk object types:

```
SOXBusEntity|SOXProcess, SOXProcess|SOXSubprocess, SOXSubprocess|SOXRisk
```

To reflect the triangle relationship shown in [Figure 76 on page 801](#), that namespace would also need to include the path between Process and Risk objects as follows:

```
SOXBusEntity|SOXProcess, SOXProcess|SOXSubprocess, SOXProcess|SOXRisk,
SOXSubprocess|SOXRisk
```

Without the configured triangle, the report author would need to use advanced techniques, which might not perform as well to accomplish this task.

To configure triangle object relationships, see [“Setting the triangle reporting framework object relationships” on page 808](#).

## Recursive object levels

You can use recursive object types to create sets of levels that are reflected in the reporting framework for use by report authors.

A *recursive object type* can have a parent object and child objects of its own type, potentially multiple layers deep. Examples of recursive object types include business entities, sub-accounts, sub-mandates, and sub-processes. For example, a business entity can have a parent business entity, such as Global Financial Services, and multiple child business entities, such as Compliance, Finance, HR, and IT, each of which can have child business entities.

The following object types are recursive within the IBM OpenPages with Watson application:

- Business Entity (SOXBusEntity)
- Sub-Process (SOXSubprocess)
- Sub-Account (SOXSubaccount)
- Sub-Mandate (Submandate)

For more information, see [“Rules for defining sets of recursive object levels” on page 803](#).

You can use recursive object levels to create a representation of corporate data that uses common names for each level of the set. The levels give the report author more context for creating reports (see [Table 245 on page 802](#)).

When the reporting framework is generated, all levels of recursive object types are reflected in the data model of the reporting framework. These structures allow report authors to create, for example, drill-down reports where users can progressively navigate through the levels to more detailed data.

For a finer level of control, you can also specify which recursive object level sets you want available in a namespace (see [“Configure reporting framework namespaces” on page 812](#)).

### Note:

- You must have at least one child object level for each recursive object level set.
- If you remove or edit child object levels in a recursive object level set, reports that use these levels will no longer run.

To configure business entity recursive object level sets, see [“Configuring business entity recursive object levels” on page 804](#).

## Example

A report author works for Global Financial Services (GFS), a large multinational bank, with an organizational structure that has many business functions and groups. The report author must create reports so business users at GFS can assess the risks that are associated with various processes that go across the company's business units. GFS organized its business around functions, divisions, departments, and units.

You might create a new recursive object level set with child levels for the Business Entity object type and name it "Organizational Hierarchy". The purpose of the new set is to return data about the various business processes and their associated risks for each organizational level of the business. The child levels are shown in the following table.

Table 245. Sample recursive object levels		
Level number	Level name	Example Business Entity instance user data
1	Group	Global Financial Services
2	Global Function	Client Markets
3	Division	Asia
4	Department	Underwriting

Table 245. Sample recursive object levels (continued)

Level number	Level name	Example Business Entity instance user data
5	Unit	Japan

After you define the business levels of the organizational structure, you need to determine which business entity is the starting point for scoping the data. In this example, you want the reporting data to start at the Global Function level. In the **Starting Entity** field, enter /Global Financial Services.

When the reporting framework is updated, a new Risk Assessment folder with the corresponding level folders and query items is created in the OpenPages\_Platform\_Reports package. The new folder is in the GRC Objects > Business Entity folder for report authors to use when they create Cognos reports.

## Rules for defining sets of recursive object levels

Rules apply to the definition of sets of recursive object levels.

You can't delete a level if it is the only level in the set. Every set must have at least one level.

The name of each user-defined level must be unique across all recursive object types.

The labels of sets and levels can be translated.

A recursive object type can repeat itself indefinitely or until some set limit is reached.

## Business Entities

A business entity is the only recursive object type where you can define multiple sets of recursive object level sets with a different starting entity for each set. Sets of Business Entity recursive object levels can also be edited and deleted.

Each set can have a different number of levels.

By default, no recursive object level sets are predefined for Business Entity object types.

Each set of recursive object levels for the Business Entity object type requires a name and a root path.

## Other object types

Sub-Process, Sub-Account, and Sub-Mandate object types have only one recursive object level set that, by default, is predefined and cannot be deleted.

By default, each of these recursive object types has a predefined first level that can only be deleted if another level has been added.

## Managing the child levels of a recursive object level set

You can add or remove levels to a recursive object level set.

**Important:** If you modify existing levels in a set, reports that used these levels will no longer run.

## About this task

To do this task, you need the **SOX > Administration > Object Types** application permission.

## Procedure

1. Click  > **Solution Configuration > Object Types**.
2. From the list of object types, click one of the following.
  - **Business Entity**
  - **Sub-Process**

- **Sub-Account**
  - **Sub-Mandate**
3. Expand **Recursive Object Levels**, and then click the recursive object level set you want to add child levels to.

The **Update Recursive Object Level** panel is displayed.

4. To remove a level from the set, click the (minus symbol) icon.

You can't delete a level if it is the only level in the set. Every set must have at least one level.

5. To add another level to the set, click **New**.

The **Add Level** panel is displayed.

Type a unique name and label for the level.

To supply translations for the label for other locales, click **Edit** and do one of the following steps:

- Enter the translation of the label for each language.

If it is displayed, click to populate translated values to the labels for display in the reporting framework. For more information, see “[IBM Watson Language Translator](#)” on page 847.

Click **Create**.

6. Update the reporting framework to apply the changes. For more information, see “[Updating the reporting framework](#)” on page 817.

## Configuring business entity recursive object levels

For the Business Entity object type, you can define and delete sets of recursive object levels, and modify the levels within each set.

By default, the Business Entity object type does not have any predefined sets of recursive object levels.

When the reporting framework is generated, all user-defined sets of recursive object levels are available to report authors under the GRC\_OBJECTS | SOXBUSENTITY\_FOLDER folder in the default namespace.

For more information, see “[Recursive object levels](#)” on page 802.

### Defining business entity recursive object levels

You can create multiple sets of recursive object levels for generation in the reporting framework.

#### About this task

To do this task, you need the **SOX > Administration > Object Types** application permission.

#### Procedure

1. Click > **Solution Configuration > Object Types**.
2. From the list of object types, click the **Business Entity** link.
3. Expand **Recursive Object Levels**, and then click **New Recursive Object Level**.
4. In the definition pane, do the following steps:

*Table 246. Entering recursive object level definition fields*

Field	Action
<b>Name</b>	Enter a name for this set of levels.
<b>Label</b>	Enter a label.
<b>Description</b>	Enter a description of this set.

Table 246. Entering recursive object level definition fields (continued)

Field	Action
<b>Starting Entity</b>	Enter the full path, beginning with a slash, to the starting Business Entity. You can use a single slash (/) to specify all top-level (Level 1) business entities.
<b>Level</b>	<ul style="list-style-type: none"> <li>a. Click <b>New</b>.</li> <li>b. Enter a unique name for this level.</li> <li>c. Enter a label.</li> <li>d. To supply translations for the label for other locales, click <b>Edit</b> and do one of the following steps: <ul style="list-style-type: none"> <li>• Enter the translation of the label for each language.</li> <li>• If it is displayed, click  to populate translated values to the labels for display in the reporting framework. For more information, see <a href="#">“IBM Watson Language Translator” on page 847</a>.</li> </ul> </li> <li>e. Click <b>Done</b>.</li> <li><b>Note:</b> If no translated text is specified, the value in the <b>Label</b> field is used by default.</li> </ul>

5. To add another level to the set, click **New**.

The **Add Level** panel is displayed.

Type a unique name and label for the level.

To supply translations for the label for other locales, click **Edit** and do one of the following steps:

- Enter the translation of the label for each language.

• If it is displayed, click  to populate translated values to the labels for display in the reporting framework. For more information, see [“IBM Watson Language Translator” on page 847](#).

Click **Create**.

the Entity Recursive Object Levels setting provides the ability to specify which recursive object level set you want available in a given namespace

6. You must configure the **Entity Recursive Object Levels** setting to specify which recursive object level set you want available in a given namespace. For more information, see [“Defining entity recursive object levels for a namespace” on page 814](#).
7. Update the reporting framework to apply the changes. For more information, see [“Updating the reporting framework” on page 817](#).

### **Deleting recursive object level sets**

You can delete a recursive object level set for a Business Entity.

**Note:** When you delete a recursive object level set for a Business Entity, all the child levels of that set are deleted. Any reports that used the deleted child levels will no longer run.

### **About this task**

To do this task, you need the **SOX > Administration > Object Types** application permission.

## Procedure

1. Click  > **Solution Configuration** > **Object Types**.
2. From the list of object types, click the **Business Entity** link.
3. Expand **Recursive Object Levels** table.
4. Click the checkbox of the set that you want to delete, and then click **Delete**.
5. Update the reporting framework to apply the changes. For more information, see “[Updating the reporting framework](#)” on page 817.

## Planning the configuration

---

You can configure numerous aspects of the reporting framework.

### Before you begin

Coordinate the configuration with your organization's IBM Cognos Analytics report writers. Working together, you can ensure that the reports you are able to produce meet the needs of your organization. You can find detailed information about designing reports in the *IBM OpenPages with Watson Report Author's Guide*.

### About this task

To configure the reporting framework, complete the following tasks:

## Procedure

1. Review the pre-defined framework models and namespaces that are provided with OpenPages. You might need to update the pre-defined namespaces or create new ones to meet your requirements.
2. Review the registry settings that apply to all framework models. For information, see “[Configuring settings that apply to all framework models](#)” on page 806.
3. Configure your own framework models and namespaces. For information, see “[Configuring framework models](#)” on page 810.
4. Configure recursive object levels. For information, see “[Configuring business entity recursive object levels](#)” on page 804.
5. Generate the reporting framework. For information, see “[Generating the reporting framework](#)” on page 814.
6. Make reports available to OpenPages users. For more information, see “[Home page, dashboard, and tabs](#)” on page 230.
7. Optional: Configure IBM Cognos Analytics dashboards and stories and make them available to end users by adding them to the home page. For information, see “[Creating a dashboard or story page](#)” on page 136.

## Configuring settings that apply to all framework models

---

The settings in the **Platform > Reporting Framework V6 > Configuration** folder apply to all framework models.

## Configuring the number of models that can be concurrently generated

The Concurrent Models setting controls how many framework models can be concurrently generated.

Generating multiple models concurrently can improve the performance of the generation process. During generation each concurrent model uses memory and CPU resources on the IBM Cognos Analytics server. Validate the impact and use caution before you increase this setting.

### Platform > Reporting Framework V6 > Configuration > Concurrent Models

Default: 2

Values: In the **Value** field, type a number.

## Including workflow fields

The Include Workflow Fields setting controls whether workflow fields are included when you generate the reporting framework.

If you do not use GRC Workflow, set Include Workflow Fields to false.

If you use GRC Workflow, set Include Workflow Fields to true to make workflow information available in the reporting framework.

For information about reporting on workflow instance data, see [“Reporting on information in workflow instances” on page 434](#).

For more information about GRC Workflow, see [Chapter 16, “Configuring GRC Workflow ,” on page 369](#).

### **Platform > Reporting Framework V6 > Configuration > Include Workflow Fields**

Default: true

Values:

- true - workflow fields are included when you generate the reporting framework.
- false - workflow fields are excluded when you generate the reporting framework.

## Adding locale codes to the reporting framework

You can add locale codes to the IBM OpenPages with Watson reporting framework so that users see localized text when they are authoring and working with reports.

### **Platform > Reporting Framework V6 > Configuration > Locales**

Default: en\_US

Values: In the **Value** field, type a comma-separated list of locale codes.

**Note:** Use only the locales that you need. Locales increase the size of the packages, which can impact performance.

You can use the following locale codes:

- en\_US (U.S. English)
- de\_DE (German)
- en\_GB (U.K. English)
- es\_ES (Spanish)
- fr\_FR (French)
- it\_IT (Italian)
- ja\_JP (Japanese)
- pt\_BR (Brazilian Portuguese)
- zh\_CN (Simplified Chinese)
- zh\_TW (Traditional Chinese)

## Defining the sort order locale

The **Sort Order Locale** setting controls the language in which query subjects and data items are sorted.

Multiple locales can be loaded into the reporting framework but the reporting framework has a static sort order based on the **Sort Order Locale** setting.

### **Platform > Reporting Framework V6 > Configuration > Sort Order Locale**

Default: en\_US

Values: In the **Value** field, type one of the following locale code values:

- en\_US (U.S. English)
- de\_DE (German)
- en\_GB (U.K. English)
- es\_ES (Spanish)
- fr\_FR (French)
- it\_IT (Italian)
- ja\_JP (Japanese)
- pt\_BR (Brazilian Portuguese)
- zh\_CN (Simplified Chinese)
- zh\_TW (Traditional Chinese)

## Setting the triangle reporting framework object relationships

To enhance report authoring capability, use the **Supported Triangle Relationships** setting to configure object types with triangle relationships in the reporting framework relational data model.

For more information, see [“Triangle object relationships” on page 801](#).

### Platform > Reporting Framework V6 > Configuration > Supported Triangle Relationships

Default: none.

Values:

**Important:** The spelling and case of the object type name must exactly match its system name. For example, type SOXBusEntity for the Business Entity object type. Using the wrong case for letters or using the label text will result in an error message.

In the **Value** box, use the following syntax to configure the three objects in a triangle relationship:

Parent1|Parent2|Child

For example:

SOXProcess|SOXSubprocess|SOXRisk

**Note:** To enter multiple sets of triangle relationships, separate each triangle set with a comma, for example:

SOXProcess|SOXSubprocess|SOXRisk, Mandate|Submandate|Requirement

## Update the reporting schema to include the triangle relationship

After you've edited the triangle objects relationships, you need to update the reporting schema.

### About this task

You can use any of the following methods:

- Run the SQL script described in this procedure. The SQL method incrementally updates the reporting schema with the triangle relationship configuration. This method is much faster than using the application user interface.
- Use the application user interface.
- Use the RpsRpfc.sh | .cmd tool.

Do this task as the OpenPages database user.

## Procedure

1. Log on to a machine with SQL\*Plus and access to the database server.
2. Run the following script:

```
Begin
 OP_CONTEXT_MGR.ENTER_SINGLE_USER_MODE;
 OP_RPS_TRIANGLE_MGR.DROP_TRIANGLE_SUPPORT;
 OP_RPS_TRIANGLE_MGR.ADD_TRIANGLE_SUPPORT;
 Commit;
 OP_CONTEXT_MGR.EXIT_SINGLE_USER_MODE;
End;
/
```

## What to do next

Regenerate the reporting framework. For details, see [“Generating the reporting framework” on page 814](#).

## Enabling the reporting framework for object types

If you've added object types and you want to run reports against them, you must include the object types in the **Object Prefix** setting. Each object type must have a unique two-letter identifier. The framework generator uses the two-letter identifier as a prefix when creating columns in the real-time reporting schema tables.

Use Z<n> as a prefix for user-created object types to avoid conflicts with future IBM OpenPages with Watson object types. Where: Z represents the first letter of the prefix, and <n> represents an uppercase letter, such as A, B, C, and so forth (for example, ZA, ZB, ZC).

### Platform > Reporting Framework V6 > Configuration > Object Prefix

Default: The pre-defined object types that are provided with OpenPages are listed.

Values: Add the new object type and prefix to the end of the current setting, with a comma as the separator. The prefix must be two uppercase letters and must be unique; no other content type in the list can have the same prefix.

In the following example, the new object type (in bold) is called CustomObject and the prefix is ‘ZA’.

```
...Obligation=OB,OblEval=OE,OblEvalValue=OV,SOXSIGNATURE=SI,CUSTOMOBJECT=ZA
```

After you set these values, update the reporting framework model. For more information, see [“Generating the reporting framework” on page 814](#).

## Defining the transaction timeout for reporting framework generation

The Transaction Timeout setting defines the processing timeout for the reporting framework generation process.

### Platform > Reporting Framework V6 > Configuration > Transaction Timeout

Default: 21600

Values: The value is in seconds.

## Defining how security checks are applied during reporting framework generation

The **Datasource QS Security Filter** setting defines how security checks are applied to query subjects during framework generation. By default, security filters are applied to the model query subjects.

### Platform > Reporting Framework V6 > Configuration > Datasource QS Security Filter

Default: False

Values:

- False: The security filter is applied to the model query subjects.
  - True: The security filter is applied to the data source query subjects.
- Changing this setting to True might impact the performance of reports.

**Note:** If you change this setting, you must regenerate the reporting framework to apply the change.

## Configuring framework models

---

Settings in an **Platform > Reporting Framework V6 > Models > [model name]** folder define one framework model. You can have multiple framework model folders.

For information about framework models, see “[Framework models](#)” on page 799.

## Creating a framework model and namespace using a template

You can use the **Template\_Model** framework model to quickly create new framework models and namespaces.

### Before you begin

Verify that the **Allow Create and Delete Settings** setting is enabled. See “[Custom settings](#)” on page 498.

### About this task

The template model contains default values for settings and one namespace, **TEMPLATE\_NAMESPACE**. To use it, you make a copy of the **Template\_Model** folder and modify the settings to meet your needs.

### Procedure

1. Click  > **System Configuration** > **Settings**.
  2. Click **Platform > Reporting Framework V6 > Models**.
  3. Select the **Template\_Model** folder.
  4. Click **Copy To**.
- The **Copy Folder To** pane opens.
5. Enter the name of the new model in **Name**. Follow the naming guidelines in “[Naming framework models](#)” on page 811.
  6. Select a folder in **Target Folder**.
  7. Click **Done**. The new folder is created.
  8. Open the new framework model folder and change the **Package Label**. Review the other registry settings and change them to meet your requirements.
  9. Expand the **Namespaces** folder in the new framework model folder. Expand the **TEMPLATE\_NAMESPACE** folder. Review the namespace registry settings and change them to meet your requirements.

## Defining a name for a framework model

Each folder under **Platform > Reporting Framework V6 > Models** defines one framework model. The name of the folder is the name of the framework model.

The names of the pre-defined framework model folders cannot be changed.

### **Platform > Reporting Framework V6 > Models > [model name]**

Default: none

Values: the name for the new framework model.

The new framework model is represented by a folder icon under the **Models** folder.

## Naming framework models

The following list contains best practices to keep in mind when naming framework models:

- Framework model names are not translated in application text.
- Use the following characters when naming framework models:
  - Lowercase letters
  - Uppercase letters
  - Numbers
  - Underscores (\_)
- Examples : Audit\_Model and RiskAssessment\_Model
- Do not use spaces.

## Defining the format for a framework model

The **Format** setting controls whether a framework model uses the standard or basic format.

For information about framework model formats, see [“Framework models” on page 799](#).

The pre-defined framework models are standard models. You cannot change the format of these models.

### Platform > Reporting Framework V6 > Models > [model name] > Format

Default: standard

Values:

- standard - the framework model uses the standard format
- basic - the framework model uses the basic format

## Enabling a framework model

The **Is Enabled** setting controls whether a framework model is available for selection in the user interface when you generate the reporting framework. If you generate all models, only enabled models are generated.

### Platform > Reporting Framework V6 > Models > [model name] > Is Enabled

Default: true

Values:

- true - when you generate the reporting framework, the framework model is available for selection in the user interface. Also, the model is generated when you choose **All Models**.
- false - when you generate the reporting framework, the framework model is not available for selection in the user interface. Also, the model is not generated when you choose **All Models**.

## Defining the query mode for a framework model

The **Mode** setting controls whether a framework model is published in Cognos using Compatible Query Mode or Dynamic Query Mode.

The **Mode** setting for the pre-defined framework models is dqm.

### Platform > Reporting Framework V6 > Models > [model name] > Mode

Default:

- IBM OpenPages with Watson: dqm
- IBM OpenPages for IBM Cloud Pak for Data: dqm

Do not change the default value. IBM OpenPages for IBM Cloud Pak for Data supports dqm only.

Values:

- dqm - the framework model is published in IBM Cognos Analytics using Dynamic Query Mode.

- cqm - Compatible Query Mode.

OpenPages does not support the generation of cqm framework models.

## Defining the package label for a framework model

The **Package Label** setting defines the package label name under which a framework model is published. Report authors see the label in IBM Cognos Analytics.

### **Platform > Reporting Framework V6 > Models > [model name] > Package Label**

Default:

Values: Type a name for the package label

Make package labels names meaningful to report authors.

## Defining whether a framework model uses profile filtering

The **Profile** setting allows you to apply the filtering functionality of profiles to the data included in the reporting framework.

If an object type in the namespace is also in the profile given in the Profile setting, only fields listed for that object type in the profile definition are included in the framework. The ResourceId, Parent Folder Id, Reporting Period Id, and Detail Page URL fields are exceptions. They are always included.

If an object type in the namespace is not in the profile, all fields are included in the reporting framework.

If the **Profile** setting is empty, all fields are included in the reporting framework.

### **Platform > Reporting Framework V6 > Models > [model name] > [profile name]**

Default:

Values: Type the name of a profile. Values are case-sensitive.

## Configure reporting framework namespaces

---

Settings in a **Platform > Reporting Framework V6 > Models > [model name] > Namespaces > [namespace name]** folder define one namespace. A framework model can have multiple namespace folders. You can copy namespace folders from one framework model folder to another framework model folder. The same namespace folder name can be used in multiple framework models.

For information about namespaces, see [“Namespaces ” on page 800](#).

The easiest way to create a new namespace is with the Template\_Model framework model. For information, see [“Creating a framework model and namespace using a template ” on page 810](#).

## Defining a name for a reporting framework namespace

Each folder under **Platform > Reporting Framework V6 > Models > [model name] > Namespaces** defines one reporting framework namespace. The name of the folder is the name of the namespace.

The names of the system-supplied namespaces cannot be changed.

### **Platform > Reporting Framework V6 > Models > [model name] > Namespaces > [namespace name]**

Default: none.

Values: name for the new namespace. For example, MY\_NS.

The new namespace is represented by a folder icon under the **Namespaces** folder.

## Naming namespaces

Names of namespaces can be translated in application text. The following list contains best practices to keep in mind when naming namespaces.

- Keep namespace names short for readability (long names will wrap to another line).
- For consistency and compatibility with the reporting framework, use only the following characters when naming namespaces:
  - Uppercase letters
  - Numbers
  - Underscores (\_)
 Examples : MY\_NAMESPACE and NAMESPACE101
- Do not use spaces.

## Defining the object model for a namespace

The **Object Model** setting is required. It contains the relationship path that is used for reporting in a namespace. A namespace cannot contain ambiguous paths.

The framework generator uses the value pairs in this setting to define the parent-child relationships in the generated framework model.

**Platform > Reporting Framework V6 > Models > [model name] > Namespaces > [namespace name] > Object Model**

Default:

Values: In the **Value** field, enter value pairs to reflect parent-child object relationships. All parent-child paths must start with SOXBusEntity. The syntax is:

```
<parent object>|<child object>, <parent object>|<child object>
```

For example:

```
SOXBusEntity|SOXProcess, SOXProcess|SOXRisk, SOXRisk|SOXControl
```

## System-supplied namespaces

If you change the **Object Model** setting in the pre-defined namespaces in the pre-defined framework model folders, the change can affect the functionality of the pre-defined reports that are supplied with OpenPages.

## Supported triangle relationships

If you want reporting capability for object types that are in a triangle relationship and have configured the **Supported Triangle Relationships** setting, the paths between these object types must be reflected in the **Object Model** setting of a namespace. The namespace can be either new or existing. For details on configuring the **Supported Triangle Relationships** setting, see “[Triangle object relationships](#)” on page [801](#).

## Configuring secondary compliance objects for basic framework models

If the namespace is used in a basic framework model, you must define allowed relationships between primary and secondary compliance objects in the **Object Model** setting.

- Secondary compliance object relationships must be added to the **Object Model** setting for the namespace, for example, SOXBusEntity | SOXIssue.
- You can define multiple relationships for a secondary compliance object, for example, SOXBusEntity | SOXIssue , SOXProcess | SOXIssue.
- Relationships between secondary compliance objects must be explicitly defined, for example, SOXIssue | SOXTask.

When the reporting framework is generated:

- Secondary compliance objects are generated like other objects but will have a hyphenated name that includes their parent object, for example, Business Entity - Issue.
- A query subject is created for each relationship defined, for example, Business Entity - Issue, Process - Issue.
- Relationships between two secondary compliance objects are generated within the context of a primary compliance object. For example, SOXBusEntity | SOXIssue, SOXIssue | SOXTask generates Business Entity - Issue and Business Entity - Issue - Action Item.

## Setting a namespace as the default

The **Is Default** setting defines whether a namespace is used as the default namespace in the OpenPages with Watson data model.

A framework model can have only one default namespace.

**Platform > Reporting Framework V6 > Models > [model name] > Namespaces > [namespace name] > Is Default**

Default:

Values:

- `true` - the namespace is set as the default namespace for use by generation logic, and is created first.
- `false` - the namespace is set as a non-default namespace.

## Enabling a namespace

The **Is Enabled** setting controls whether a namespace is generated when you generate the reporting framework.

**Platform > Reporting Framework V6 > Models > [model name] > Namespaces > [namespace name] > Is Enabled**

Default: `true`

Values:

- `true` - the namespace will be generated when the framework model is updated.
- `false` - the namespace will not be generated and any previously existing namespace will be removed.

## Defining entity recursive object levels for a namespace

If one or more sets of recursive object levels are defined in the OpenPages with Watson application, the Entity Recursive Object Levels setting provides the ability to specify which recursive object level set you want available in a given namespace.

**Platform > Reporting Framework V6 > Models > [model name] > Namespaces > [namespace name] > Entity Recursive Object Levels**

Default:

Values: Multiple recursive object level sets must be separated by a comma. For example:

ROL-1, ROL-2, ROL-3

For information on defining recursive object levels, see [“Recursive object levels” on page 802](#).

## Generating the reporting framework

When you generate the reporting framework, the packages for all or selected framework models are published to the Cognos server with relationship subnamespaces.

Do not use IBM Cognos Framework Manager to modify the packages. The packages are created and re-created dynamically when you generate the reporting framework in OpenPages. If you made changes using IBM Cognos Framework Manager, those changes are lost when you generate the reporting framework. If you want to create a custom Cognos package, see your OpenPages consultant.

## Regenerating the reporting framework

The following table lists the actions that require the reporting framework to be regenerated. In some cases, the reporting schema must also be re-created

<i>Table 247. Re-creating the reporting schema and regenerating the reporting framework</i>			
<b>This type of change...</b>	<b>Requires this action...</b>		
	<b>Generate reporting schema</b>	<b>Update reporting schema</b>	<b>Generate reporting framework</b>
Adding a new field to a field group.	No	No	Yes
Adding a new object type.	No	No	Yes
Adding a new association between object types.	No	No	Yes
Removing object types or attributes.	Yes	No	Yes
Encrypting a long string (CLOB) field.	No	No	Yes
Defining, modifying, or deleting business entity recursive object levels.	No	No	Yes
Removing a field from a field group.	No	No	Yes
Disabling an association between object types.	No	No	Yes
Changing the security model.  <b>Note:</b> Changing the security model after data is loaded or migrated into the system is not recommended and requires assistance from the OpenPages Support team.	Yes	No	Yes
Changing the value of the <b>Populate past periods</b> setting.  For more information, see “ <a href="#">Populating past reporting periods</a> ” on page 119.	Yes	No	No
Changing any setting used to compose URL links in the reporting schema, for example, the Host, Port, and Protocol settings.  To update the reporting schema by running the RPS_Update SQL script, see “ <a href="#">Updating URL host pointers for reports</a> ” on page 633. To update the reporting schema by using the UI, see “ <a href="#">Updating the reporting schema</a> ” on page 121.	Yes	No	No

*Table 247. Re-creating the reporting schema and regenerating the reporting framework (continued)*

<b>This type of change...</b>	<b>Requires this action...</b>		
	<b>Generate reporting schema</b>	<b>Update reporting schema</b>	<b>Generate reporting framework</b>
Adding an index to an RT_column by using the <b>Settings &gt; Platform &gt; Reporting Schema &gt; Create Index on Fields</b> setting.	No	Yes	No
Setting or changing the display type of a field to Multi-Valued User Selector or Multi-Valued Group Selector or Multi-Valued User Group Selector.	No	Yes	No
Importing a profile by using ObjectManager or the <b>Import Configuration</b> feature.	No	Yes	No
Configuring the triangles setting. For more information, see “ <a href="#">Triangle object relationships</a> ” on page 801.	Yes	No	No

**Important:** After you regenerate the reporting framework, test the reports.

## Reporting framework permissions

Before you do any actions on a reporting framework, you must have specific application permissions set on your account.

For more information, see “[Types of application permissions](#)” on page 52).

*Table 248. Reporting framework permissions*

<b>This application permission...</b>	<b>Is used to...</b>
Reporting Framework	Update the reporting framework. The Reporting Framework permission enables the  > <b>Cognos Analytics &gt; Reporting Framework Generation</b> menu item.

## Choosing update options in the reporting framework

When you generate the reporting framework, you can choose to update all models or selected models.

The Legacy Reporting Framework cannot be generated.

[Table 249 on page 816](#) lists the various options for updating the reporting framework.

*Table 249. Reporting Framework Generation Options*

<b>This option...</b>	<b>Does this...</b>
All Models	Generates all framework models that are enabled. For each model, the framework model, labels (object text), and custom query subjects are generated.

Table 249. Reporting Framework Generation Options (continued)

This option...	Does this...
Selected Models	Generates the models that you select. For each model, the framework model, labels (object text), and custom query subjects are generated.  The list displays all framework models that are enabled.

When you update the reporting framework, any changes to the reporting schema are reflected in Cognos. After the reporting framework model in Cognos is updated, report authors can create and modify reports based on these changes. If the reporting framework is not updated, external reports such as those built with Cognos will not be able to access the updated reporting schema.

### Example

You add two new fields to a Risk object type and add a new child or parent relationship to a Control object type. You also want users to be able to run reports that contain these new fields or relationships.

To make these changes available to a report author in Cognos, you must update the reporting framework.

After the Cognos reporting framework is updated, a report author can then create new (or modify existing) reports that contain the new fields or relationships. For more information about the Cognos reporting framework, see the *IBM OpenPages Report Author's Guide*.

## Updating the reporting framework

After the reporting schema has been re-created, the reporting framework must be updated as well to propagate the changes to Cognos.

### About this task

To do this task, you need the **SOX > Administration > Reporting Framework**.

**Note:** You can also generate the reporting framework by using the command line. For more information, see [“Generating the reporting schema and framework from a command line” on page 121](#).

### Procedure

1. Click  > **Cognos Analytics > Reporting Framework Generation**.
2. Click **Update**.
3. Complete the options on the Reporting Framework Generation page. For more information, see [“Choosing update options in the reporting framework” on page 816](#).
4. Click **Submit**.

### What to do next

Review the results. For more information, see [“Viewing reporting framework details” on page 817](#). Test the reports.

## Viewing reporting framework details

You can view the details of a refresh operation and review any errors.

### Procedure

1. Click  > **Cognos Analytics > Reporting Framework Generation**.
2. On the **Reporting Framework** tab, use the search box to find the operation that you want to view.
3. Click the name of the operation.

A summary page opens with two tabs, **Information** and **Log**.

4. Click the **Information** tab to view information about the operation.  
If suboperations exist, they are listed in on the **Suboperations** pane.
  - a) To view suboperation details, click the name of the suboperation.
  - b) To view log details, click **View Log**.
5. Click the **Log** tab to view log messages for an operation or suboperation.

# Chapter 30. IBM OpenPages with Watson connectors

You can leverage information from across the business by using connectors to collect information from third-party solutions.

IBM OpenPages with Watson connectors use IBM Security Directory Integrator (SDI) to pull data into OpenPages.

Security Directory Integrator is a general-purpose integration tool that you can use to build integrations between multiple data sources and targets. Connectors must be imported into a Security Directory Integrator workspace. (IBM Security Directory Integrator is the latest name for IBM Tivoli® Directory Integrator.)

The version included in the IBM OpenPages with Watson installation media is Security Directory Integrator 7.2.0.6. This version is supported by the QRadar® integration package and by IBM OpenPages SDI Connector for UCF Common Controls Hub.



**Attention:** Security Directory Integrator must be at the 7.2.0.6 level.

## IBM QRadar integration

IBM OpenPages with Watson includes an IBM QRadar integration package. QRadar is a separate stand-alone enterprise-level application. It is not included with IBM OpenPages with Watson.

IBM QRadar is a SIEM (Security Information and Event Management) system that contains relevant data for the Incident object type in OpenPages. In QRadar, this data is called an Offense.

Data can be pulled from QRadar, initiated by IBM Security Directory Integrator (SDI), then mapped one-to-one to Incidents in IBM OpenPages with Watson.

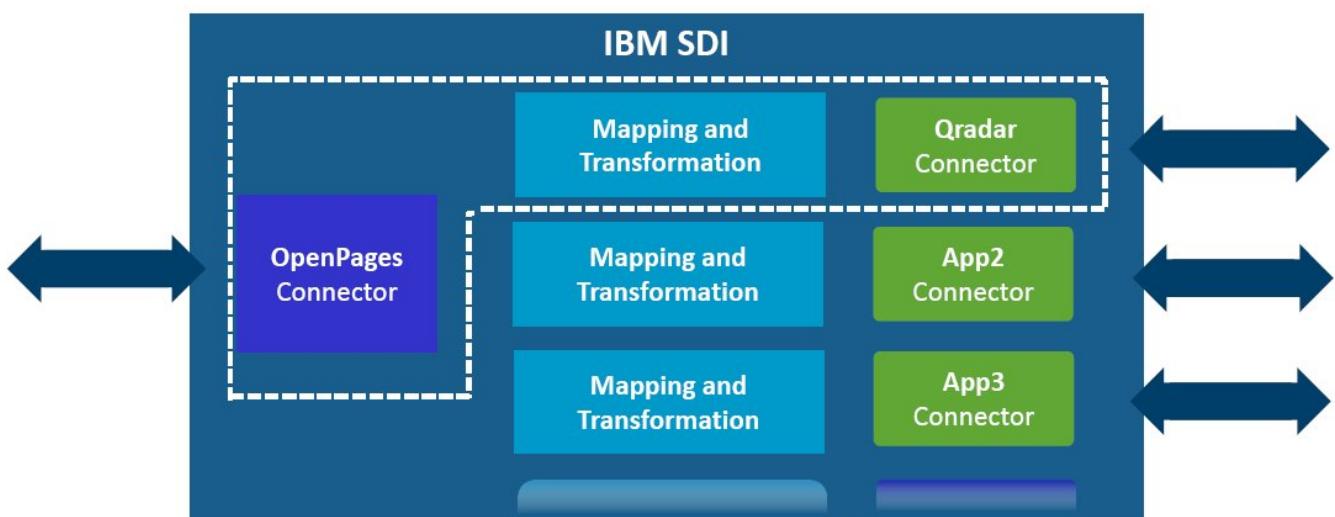


Figure 77. How OpenPages and QRadar work together

# Using the QRadar integration project

The IBM QRadar integration project is an optional project that you can install to import Offenses from QRadar and create them as Incidents in the IBM OpenPages with Watson.

## Before you begin

You must complete the following steps to install and configure the QRadar integration project before you begin. For more information, see "Installing QRadar integration" in the *IBM OpenPages with Watson Installation and Deployment Guide*.

## About this task

Connectors are plug-ins for SDI that are reusable components. OpenPages has one connector developed for OpenPages functionality. The connector is generic to any OpenPages object type and field type.

You can use QRadar filtering so that the relevant subset of Offenses can be managed in the context of the impact on your business. For example, you can configure the connector to import only Offenses that are open, or based on the date.

The SIEM API documentation is available in the QRadar Console. This can provide guidance on what to specify for the filter and the fields, (specified by the **qradarFilter** and **qradarFields** properties in the connector.properties file).

## Procedure

1. Ensure IBM QRadar is installed. IBM QRadar is a separate enterprise-level application. It is not included with OpenPages.
2. Install IBM Security Directory Integrator 7.2, then install pack 6. The installation files are available in the OpenPages installation media.
3. Configure Security Directory Integrator to connect to QRadar.
4. Configure the property files.
5. Deploy the assembly line.



**Attention:** The assembly line will not run when the OpenPages user that is configured to run the assembly line has left System Admin Mode enabled in OpenPages. You must ensure that System Admin Mode is disabled to run the assembly line. To disable System Admin Mode, click **Events > Disable System Admin Mode**.

6. The results of running the assembly line show up as new or updated Incident objects. To view them, click **Events > Incidents** in OpenPages.

## Configuring email notifications to be sent from the QRadar assembly line connector components

Both of the QRadarOffensesToIncidents assembly line connector components are able to send email notifications to alert people such as the IBM Security Directory Integrator (SDI) administrator when errors or exceptions occur during the execution of the QRadarOffensesToIncidents assembly line.

## About this task

To enable this capability, the three SMTP properties in the connector.properties file must be configured. Then, when an error or exception occurs, in addition to the error-level message getting logged to the SDI log file or to the SDI console, an email with the log message is also sent to the email addresses configured in the SMTP **mailto** property of the connector.properties file.

Email messages can be sent from either the QRadar API connector component or the IBM OpenPages with Watson connector component of the QRadarOffensesToIncidents assembly line. Also, the IBM OpenPages with Watson connector automatically sends warn-level messages if there are issues with the

validity of the primary parent ID supplied to the IBM OpenPages with Watson connector when attempting to create a new IBM OpenPages with Watson object. Updating an existing IBM OpenPages with Watson object does not require a primary parent ID to be specified.

## Procedure

1. Configure the **mailto** property of the connector.properties file.

The email address to use for sending email notifications about errors and exceptions that occur in the assembly line connectors. You can specify one or more email addresses by typing a comma-separated list. For example, **mailto=user1@acme.com,user2@acme.com**.

2. Configure the **smtpPort** property of the connector.properties file.

The SMTP port to use for sending email notifications about errors and exceptions that occur in the assembly line connectors. The default port to use for an SMTP server is 25.

3. Configure the **smtpHost** property of the connector.properties file.

The SMTP host to use for sending email notifications about errors and exceptions that occur in the assembly line connectors. Specify either an IP name or IP address. For example, **smtpHost=mySmtpHost.acme.com** or **smtpHost=192.168.10.20**.

## Specifying a primary parent ID to the OpenPages connector

IBM OpenPages with Watson objects that are created by the OpenPages connector must have a primary parent ID.

## Procedure

There are three ways to supply a primary parent ID to the OpenPages connector component, described in the order in which they are searched for:

- Provide the object resource ID of an existing suitable parent object as a string value in the **work.primary\_parent\_id** property in the output mapping:

The following graphic shows the **work.primary\_parent\_id** property in the output mapping:

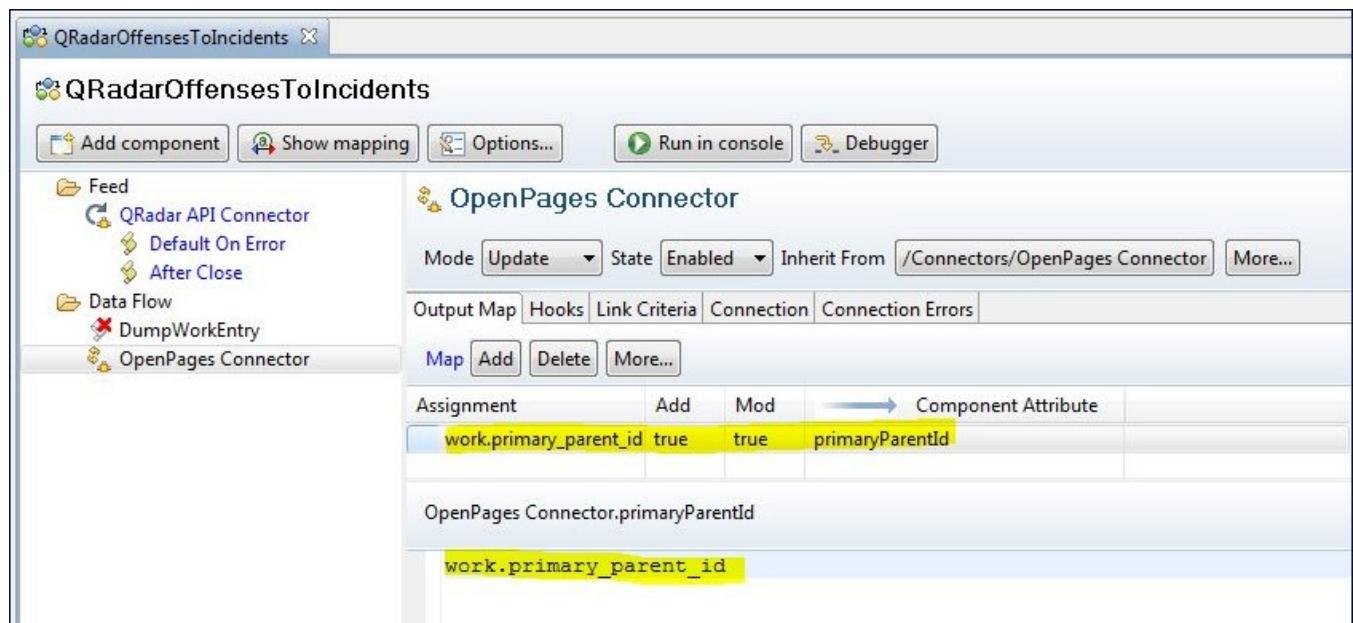


Figure 78. The **work.primary\_parent\_id** property in the output mapping:

The value must be a number, enclosed in double quotes, and should be the object resource ID of a suitable OpenPages parent object. A null or empty value is ignored. This technique enables the use of a different primary parent ID for each object being created.

- If a **work.primary\_parent\_id** property value is not supplied in the OpenPages connector output mapping from the preceding technique, then the OpenPages connector looks for non-null values of the following two properties in the output mapping to derive the primary parent ID of a parent object for the new object being created:
  - work.parent\_type**: the OpenPages object type of the parent object
  - work.parent\_location**: the relative location of the OpenPages parent object instance

The following graphic shows the primary parent ID derived from the non-null values of the two properties **work.parent\_type** and **work.parent\_location** in the output mapping.

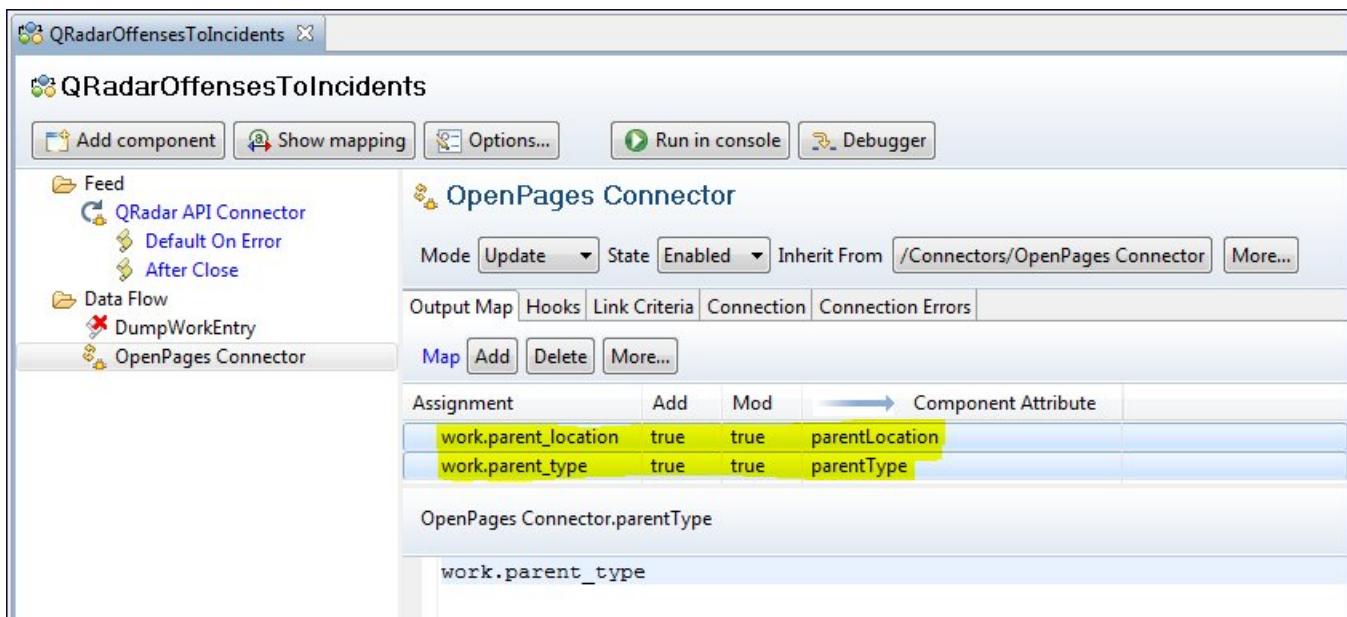


Figure 79. Primary parent ID derived from the non-null values of the two properties **work.parent\_type** and **work.parent\_location** in the output mapping

See the detailed descriptions and example values provided for the **op\_parentType** and **op\_parentLocation** properties in the connector.properties file, located in the Runtime-qradar\_integration folder of the SDI qradar\_integration project. If the values for these properties do not derive to a valid parent object, then they are ignored.

The following graphic shows a detail from the connector.properties file:

```

op_parentType
#
The GRC object type of the parent object to use for all newly created objects.
#
Example: op_parentType=SOXBusEntity
op_parentType=SOXBusEntity

#
op_parentLoc
#
The relative location of the GRC parent object instance to use as the parent for all
newly created objects. For Business Entity parents, specify all of the segments of the
Folder location except for the root. For non-Business Entity parents, specify all of
the segments of the folder location except for the root and append the name of the parent
object as the last segment of the location. The op_parentLoc property should start with
a leading '/' character; do not include any spaces around the '/' characters.
#
Example 1: If a business entity object named 'Audits' has a Folder value of
BusinessEntity / Library / Audits
then specify the relative location, that is, just the segments of the pathname under the
root folder (in this case the root folder is 'BusinessEntity'), as follows:
opParentLoc=/Library/Audits
#
Example 2: If a business entity object named 'Asia Pacific' has a Folder value of
BusinessEntity / Global Financial Services / Asia Pacific
(where 'BusinessEntity' is the root in the Folder property) then specify the property as:
op_parentLoc=/Global Financial Services/Asia Pacific
#
Example 3: If a non-business entity Risk object named 'Risk1' has a Folder value of
Risks/test1
(where 'Risks' is the root in the Folder property) then specify the property as
follows, being sure to append the parent object's name (in this example the parent
object's name is 'Risk1'):
op_parentLoc=/test1/Risk1
#
op_parentLoc=/Library/Audits

```

Figure 80. A detail from the connector.properties file

This technique enables the use of a different primary parent ID for each object being created.

- If the properties in the preceding two techniques are not provided, then the OpenPages connector uses the default primary parent ID derived from the **op\_parentType** and **op\_parentLocation** properties defined in the connector.properties file, located in the Runtime-qradar\_integration folder of the SDI qradar\_integration project. The values in the connector.properties file are processed once per assembly line execution, and the resulting derived value serves as the default primary parent ID to use if the properties in the two preceding sections are not provided.

If the values for these properties do not derive to a valid parent object, then there will be no default value available for the duration of the assembly line execution. See the detailed descriptions and example values provided for each of these properties in the connector.properties file, located in the Runtime-qradar\_integration folder of the SDI qradar\_integration project.

## Specifying currency values to the OpenPages connector by the output mapping

You can specify currency values in the IBM OpenPages with Watson connector output mapping as strings (enclosed with quotation marks) by using a standard format.

### About this task

The amount is specified first, followed by a vertical bar, followed by the ISO code. White space is allowed. The entire string must be enclosed in quotation marks.

### Procedure

Supply the currency values in the OpenPages connector output mapping as strings, that is, enclosed with quotation marks, by using the following format: "<amount>|<isoCode>"

- Examples of valid currency values in the output mapping: "123.45|AUD" or "321 | USD"
- Example of an invalid currency value in the output mapping because the enclosing quotation marks are missing: 123.45|AUD
- Example of an incomplete currency value in the output mapping because the ISO code is missing; when this situation occurs, the default currency that is configured in OpenPages is used: "123 | "

## Specifying date values to the OpenPages connector via the output mapping

Date values should be specified as **java.util.Date** objects in the IBM OpenPages with Watson connector output mapping.

## IBM OpenPages SDI Connector for UCF Common Controls Hub integration

You can use IBM OpenPages SDI Connector for UCF Common Controls Hub to bring data from UCF Common Controls Hub into OpenPages. UCF Common Controls Hub is a separate stand-alone web application. It is not included with OpenPages.

UCF is a database of regulatory compliance documents. The regulatory documents are divided into parts, which can then be used by APIs. UCF Common Controls Hub is the web portal to the UCF data.

Data can be pulled from UCF (initiated by IBM Security Directory Integrator), then mapped one-to-one to object types in OpenPages.

**Note:** IBM Security Directory Integrator is the latest name for IBM Tivoli Directory Integrator.

*Table 250. UCF object type mappings*

Object type in UCF	Object type in OpenPages
Authority documents	Mandates
Citations	Sub-Mandates
Controls	Requirements

A mandate can have one or more sub-mandates. A sub-mandate can have zero or more requirements. A requirement can be related to multiple sub-mandates from different mandates.

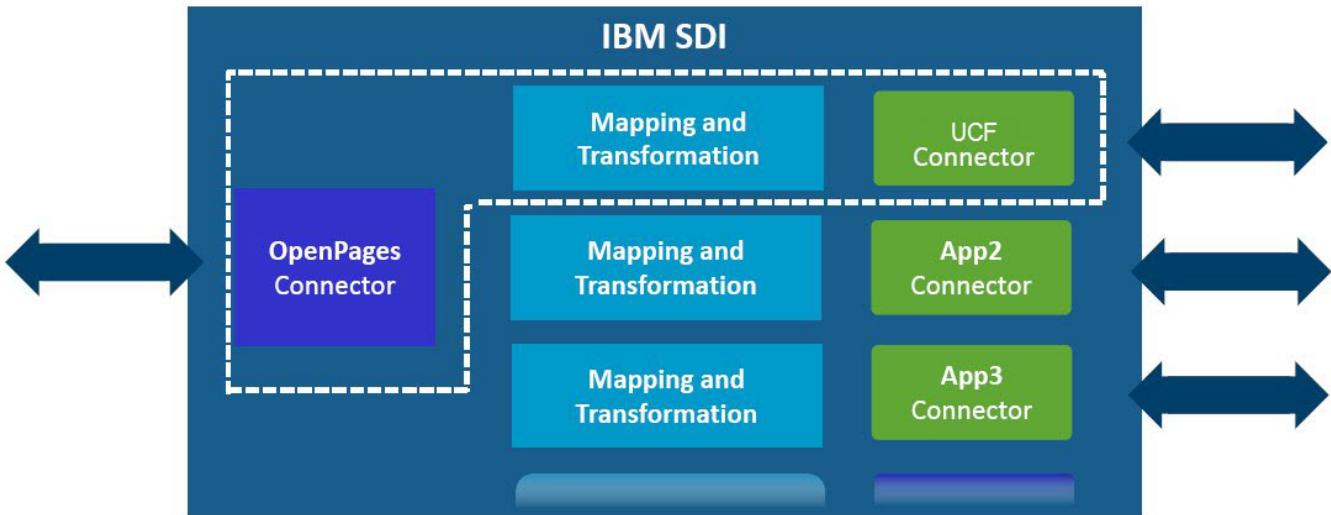


Figure 81. How OpenPages and UCF work together

## Run the UCF assembly lines

Run the UCF assembly lines to import objects from UCF Common Controls Hub into OpenPages.

You must install and configure the UCF connector before you begin. For more information, see "Installing UCF integration" in the *IBM OpenPages with Watson Installation and Deployment Guide*.

Run the assembly lines in the following order. Wait for each assembly line to finish before you run the next assembly line:

- UCF Authority Documents to OP Mandates
- UCF Citations to OP Submandates
- UCF Controls to OP Requirements

To run an assembly line, right-click it in the **SDI Configuration Editor** and click **Run AssemblyLine**. To view the log, click .

**Note:** The UCF connector assembly lines do not support Delta mode.

You can schedule the assembly lines to run by using the IBM Security Directory Integrator scheduler. Set up the scheduler so that each assembly line completes before the next begins.



**Attention:** The assembly lines will not run when System Admin Mode (SAM) is enabled in OpenPages. The assembly lines write data to the OpenPages database, and System Admin Mode prevents write operations. Ensure that System Admin Mode is disabled before you run the assembly lines. To disable System Admin Mode, click  > **Disable System Admin Mode**.

To view the UCF objects in OpenPages, go to **Compliance > Mandates**. Click **Library > UCF**.

## Updating connection information

If you need to update the connection information that the UCF connector uses to connect to OpenPages or to UCF Common Controls Hub, see "Configuring connection information" in the *IBM OpenPages with Watson Installation and Deployment Guide*

## Troubleshooting

If an assembly line fails the first time that you run it, open IBM Security Directory Integrator, click the icon to restart the default server, and then run the assembly line again.

If you encounter errors about missing impact zones or guidance areas, update the UCF fields with the new enumerated string values. See "Update business entities and fields" in the *IBM OpenPages with Watson Installation and Deployment Guide*

## IBM Security Directory Integrator (SDI) techniques

---

If you use the IBM OpenPages with Watson connectors, there are SDI techniques that might help you.

### Scheduling Security Directory Integrator

IBM Security Directory Integrator (SDI) has a built-in capability for scheduling. Each assembly line can have one or more schedules. SDI can run in a daemon mode between runs, or shut down completely. Assembly lines can also be run on demand by the command line.

In the SDI Configuration Editor, right-click an assembly line and select **Create Schedule**.

If you are using the UCF connector, schedule the assembly lines in the following order. Schedule the assembly lines so that each completes before the next begins.

- UCF Authority Documents to OP Mandates
- UCF Citations to OP Submandates
- UCF Controls to OP Requirements

For more information about scheduling assembly lines, see [IBM Security Directory Integrator Scheduler](#) in the Security Directory Integrator documentation.

### Security Directory Integrator command line tips

You can run the assembly lines on your local or remote server where IBM Security Directory Integrator (SDI) is installed.

To run commands on a remote SDI server, you must have SDI installed on your local system. When entering SDI commands on the local server to execute on a remote SDI server, be sure to include the **-h <hostname>** command switch.



#### Attention:

- If changes are made to any of the properties files that are used by the connector components and you are running SDI as a service, the service must be stopped and restarted for those changes to take effect.
- Logging for SDI running as a service is written to the ibmdi.log file in the installed SDI area where the service lives. For example, on a Windows-based system, this is <SDI-install-root>/win32\_service/logs/ibmdi.log by default.
- When you run an assembly line by using the SDI Configuration Editor, the log entries are put into the <SDI-solutions-root>/logs/ibmdi.log by default.

Here are some examples of commands that you can run against your imported configuration. Note the use of the **-h <hostname>** switch when the command is intended to run on a remote SDI server configuration. Also, the use of the **ibmdisrv** command is not typically used, but is included here as an example of how it can be used.

In these examples, the QRadar integration is located inside the SDI workspace at the following location: C:\SDI\_Solutions\workspace\qradar\_integration\Runtime-qradar\_integration\qradar\_integration.xml.

- tdisrvctl -v -op start -c C:\SDI\_Solutions\workspace\qradar\_integration\Runtime-qradar\_integration\qradar\_integration.xml -r QRadarOffensesToIncidents
- tdisrvctl -v -h <hostname> -op start -c C:\SDI\_Solutions\workspace\qradar\_integration\Runtime-qradar\_integration\qradar\_integration.xml -r QRadarOffensesToIncidents

- `ibmdisrv -c "C:\SDI_Solutions\workspace\qradar_integration\Runtime-qradar_integration\qradar_integration.xml" -r "QRadarOffensesToIncidents"`

## Troubleshooting the assembly line "Connection refused" error

When you start the IBM Security Directory Integrator (SDI) Configuration Editor, or when you run SDI commands from a command line, you might encounter an error that says the connection to your SDI server is refused.

### About this task

This error can be caused by running more than one instance of either the SDI Configuration Editor or the SDI service at the same time on the same server.

### Procedure

1. Check for any program that is using port 1099 already by using the following commands:
  - Windows: `netstat -an | findstr 1099`
  - Linux: `netstat -an | grep 1099`
2. If the output of this command is not empty, determine which process is already using port 1099 and stop that process. If the process is already stopped, re-enter the command after a minute or two to ensure that the ports are no longer in use. You might need to repeat the **netstat** command a few times before the output is empty.



# Chapter 31. Configuring questionnaire assessments

You can use the questionnaire assessments to assess risk and compliance or to collect information for specific processes and asset risks. This capability streamlines, standardizes, and centralizes the collection of questionnaire-based assessment information.

To use questionnaire assessments, you set up user permissions for users. You can also configure the email server so that the workflow send emails to assignees. You can customize two visual elements on questionnaire assessments: the logo in the header and the introduction text on the landing page. These elements are displayed on all questionnaire assessments regardless of the questionnaire template and program that is used to create the questionnaire assessments.

For more information about customizing the logo and the introduction text, see *Editing a questionnaire template* in the *IBM OpenPages with Watson User Guide*.

## Before you begin

Questionnaire assessments move through a review process. The review process is based on GRC Workflow.

Determine what questionnaire assessment workflow is used to drive the review process. OpenPages includes an out-of-the-box Questionnaire Assessment Workflow. You can use it as is, modify it to meet your needs, or create your own workflow.

Lifecycle fields control behavior in the questionnaire UI. Study the Questionnaire Assessment Workflow. Look at how it sets the following lifecycle fields:

- OPLC-QAssessment:LCStage - sets a stage to Information Gathering, Review, or Approval
- OPLC-Std:LCReadOnly - makes answers read only or not
- OPLC-Std:LCInReview - adds ability to reject or accept answers
- OPLC-QAssessment:LCName - specifies the lifecycle to use

LCStage is a required field. If you create your own workflow, LCStage must be set to Information Gathering for the initial stage. For later stages, setting LCStage is optional.

LCReadOnly and LCInReview fields can be used to render the questionnaire assessment at each stage.

Questionnaire assessments and programs must be assigned a lifecycle in LCName. A lifecycle can be two-stage, three-stage, or four-stage.

If you create your own workflow, set these fields as a questionnaire assessment moves through the workflow stages. Be sure to review who the questionnaire assessment is assigned to at each stage.

The workflow controls the options on both the **Action** button in the Questionnaire Assessment Task View and the **Action** button in the questionnaire UI. The options remain synchronized and the same throughout a workflow. A workflow can be advanced by clicking the button in either the Task View or the questionnaire UI. However, it is a best practice to use the button within the questionnaire UI.

For more information about GRC Workflow, see [Chapter 16, “Configuring GRC Workflow ,” on page 369](#).

## Procedure

1. Configure the email server that is used to route emails to assignees. For information see [“Configuring your mail server” on page 486](#).
2. Verify that users who create and launch programs have the following permissions:
  - Read/write/associate access to Questionnaire Template objects.
  - Read/write access to the objects used by Questionnaire Templates: Section Templates, SubSection Templates, and Question Templates.

- Read/write/associate access to Program objects.
  - Read/write/associate access to Questionnaire Assessment objects.
  - Read/associate access to assets.
  - Lock/unlock permissions on files.
3. Verify that users who complete and review questionnaire assessments have the following permissions:
- Read access to the objects used by questionnaire templates: Questionnaire Templates, Section Templates, SubSection Templates, and Question Templates.
  - Read access to Program objects. Required for four-stage lifecycle because the program owner is at one point the assignee for questionnaire assessments.
  - Read/write/associate access to Questionnaire Assessment objects. You can do this with Record Level Security (RLS), where the current assignee has the questionnaire assessment, or with the role template.
  - Read/write/associate/delete access to SOXDocument for attachments.
  - Read access to assets.

# Chapter 32. Configuring OpenPages Loss Event Entry

IBM OpenPages Loss Event Entry is an optional, chargeable component that users across an organization can access to create loss events. You can customize the app by configuring how it works for your organization, and the way users view and interact with it. OpenPages Loss Event Entry can be used to create only loss events together with loss impacts, loss recoveries, and files. You cannot use it to create other object types.

You use  > **Integrations** > **Loss Event Entry App** to configure the OpenPages Loss Event Entry app. For more information, see [“Configuring the Loss Event Entry app” on page 839](#). Review that topic to learn about how to configure OpenPages Loss Event Entry.

Read [“Planning the configuration ” on page 831](#) to learn about whether you can use the out-of-the-box configuration that is included in OpenPages Loss Event Entry. If you choose to modify the out-of-the-box configuration, the following topics explain aspects of the system you need to understand before you begin:

- [“Designing the loss entry form for the Loss Event Entry app” on page 833](#)
- [“How users are handled” on page 833](#)
- [“Where loss events get created” on page 833](#)
- [“Who loss events get assigned to ” on page 834](#)
- [“How dates are validated” on page 835](#)
- [“How to launch OpenPages Loss Event Entry ” on page 835](#)
- [“How confirmation emails are configured” on page 837](#)

## Planning the configuration

You can use OpenPages Loss Event Entry either as it is out-of-the-box with a minimal amount of configuration or you can make modifications for your organization.

To use OpenPages Loss Event Entry as it is out-of-the-box, you need to complete the following configuration tasks:

1. In  > **Integrations** > **Loss Event Entry App**, change the passwords of the dedicated users that are included in OpenPages Loss Event Entry. For information, see [“Configuring the Loss Event Entry app” on page 839](#).
2. Review the creation views for loss events and decide whether you want to display or hide the **Loss Impacts** and **Loss Recoveries** tabs. If displayed, you can also decide whether to make them mandatory. Creation views are described later in this topic. How you can make the tabs mandatory is described in [“Configuring the Loss Event Entry app” on page 839](#).
3. Change the role template assignment for the **Loss Event Entry** role template so that it grants the lowest level of access needed.
4. In the **Loss Event Entry App** page, define **Default Parent Path** and **Default Triage Team**. For information, see [“Configuring the Loss Event Entry app” on page 839](#).
5. Place a URL on your organization's intranet. For information, see [“How to launch OpenPages Loss Event Entry ” on page 835](#).
6. Recommended: Enable auto-naming for the Loss Event, Loss Impact, and Loss Recovery objects. Although not required, it prevents failures due to duplicate names and inconsistencies in user-given names. Users who create loss events do not know the naming rules in OpenPages.

You can, optionally, modify many aspects of OpenPages Loss Event Entry. To do this, review what is included in the system and modify any of the following items to meet your requirements:

- Decide what locales you need. It is a best practice to disable locales that you do not use and disable the dedicated users for them.
- Review the user group, `Loss_Event_Entry`, and make changes if needed. It contains ten dedicated users, one for each locale: `LEE_EN_US`, `LEE_EN_GB`, `LEE_IT_IT`, `LEE_PT_BR`, `LEE_FR_FR`, `LEE_ES_ES`, `LEE_DE_DE`, `LEE_ZH_TW`, `LEE_ZH_CN`, and `LEE_JA_JP`. For more information, see “[How users are handled](#)” on page 833.
- Review the role template, `Loss_Event_Entry`, and make changes if needed. The ten dedicated users are assigned to this role template at the root business entity. It is a best practice to change the role template assignment for the `Loss_Event_Entry` role template so that it grants the lowest level of access needed.
- Review the profile, `Loss_Event_Entry`, and make changes if needed. The ten dedicated users are assigned to this profile.

You must use the `Loss_Event_Entry` profile. It's the only profile that is supported by the Loss Event Entry app.

- Design the content of the loss event form. For more information, see “[Designing the loss entry form for the Loss Event Entry app](#)” on page 833.
- Review the field groups, `OPSS-LE-BE` and `OPSS-LE-Contact`. `OPSS-LE-BE` contains Business Entity Selector fields that are used to identify the involvement of business entities in loss events. `OPSS-LE-Contact` contains fields that contain user information such as name, email, and phone number.
- Review the date validation rules that are included in the system and make changes if needed. You configure date validation rules in the **Loss Event Entry App** page. For information, see “[How dates are validated](#)” on page 835.
- Determine how you want to set the parent business entity. For information, see “[Where loss events get created](#)” on page 833. Fields that contain parent business entities must be of the display type, Business Entity Selector.
- Determine how you want to set the assignee for new loss events (the triage team).

If you want users to select the assignee for new loss events, add a user or group selector field to the Loss Event creation view.

For information, see “[Who loss events get assigned to](#)” on page 834.

- Customize the informational text that is displayed in the Loss Event Entry app:

- To change the text that displays when users click the  icon for the Information box in the header, change the text associated with the Application Text key, `loss.event.entry.overall.help`.
- To change the information that is displayed at the top of the tab for each object type, change the text for the keys, `loss.event.entry.file.intro`, `loss.event.entry.loss.event.intro`, `loss.event.entry.loss.impact.intro`, and `loss.event.entry.loss.recovery.intro`.
- Customize the logo on the **Loss Event** form to be your company logo. File specifications are as follows:
  - Size: 1130 pixels wide by 36 pixels high
  - Name: `Logo.png`
  - Folder location: `../taskui.war/image/lossevent/`

Changes to the logo file can be overwritten in subsequent upgrades.

- Design and configure the email confirmation that is sent to users when a loss event is created. For information, see “[How confirmation emails are configured](#)” on page 837.

## Designing the loss entry form for the Loss Event Entry app

---

The loss entry form that users see when they open OpenPages Loss Event Entry is controlled by system views, which are provided with OpenPages. You can use the default views or create your own.

By default, Loss Event Entry uses the following creation views:

- SysView-New-LossEvent-LEE
- SysView-New-LossImpact-LEE
- SysView-New-LossRecovery-LEE

These views are assigned to the **Loss Event Entry** profile. The views determine what tabs and fields are displayed in Loss Event Entry.

If you want to change the views, do the following steps:

1. Build a creation view for the object type: Loss Event, Loss Impact, or Loss Recovery. See [“Defining a Creation View” on page 263](#).

For example, you can create a new creation view for Loss Events by using the following options:

- On the **Overview** tab, set:
    - **Object type:** Loss Event
    - **Type:** Creation
    - **Copy from view:** SysView-New-LossEvent-LEE
  - On the **Rules** tab, set:
    - **View priority:** 1
    - **Profiles:** Loss Event Entry
2. Decide whether you want to display or hide the **Loss Impacts** and **Loss Recoveries** tabs. If you want to display these tabs in creation views that you create, they must be defined as child views on the Loss Event creation view.
  3. Assign the view to the **Loss Event Entry** profile.

## How users are handled

---

Users can create loss events in OpenPages Loss Event Entry without a user account for OpenPages. A dedicated user group that includes ten dedicated users, one for each supported locale, is included in OpenPages Loss Event Entry. When users access OpenPages Loss Event Entry, they do not need to enter a user ID and password. The system automatically logs them in to OpenPages Loss Event Entry with the dedicated user associated with the locale.

Users with access to OpenPages can create loss events as they always have or choose to use OpenPages Loss Event Entry. However, OpenPages users cannot log in to both at the same time in the same browser. Instruct your OpenPages users that they must log out of OpenPages when they want to use OpenPages Loss Event Entry. If you want to force OpenPages users to use IBM OpenPages Loss Event Entry, you can add Loss Event to the list of objects that are disabled for **New**. For more information, see [“Controlling the availability of object types with the New button on Grid Views” on page 213](#). Additionally, the profile and role template assignments for OpenPages users is disregarded when they use OpenPages Loss Event Entry.

## Where loss events get created

---

Loss events must be assigned to a parent business entity within the organization. You determine how this assignment is made when you define **Default Parent Path** and **Parent Field Name** in the **Loss Event Entry App** page.

For information, see [“Configuring the Loss Event Entry app” on page 839](#).

You can choose one of the following methods:

- Static: your organization assigns all loss events to one default business entity. The triage team then reassigns them to the correct business entities. To use this method, you enter the default business entity in **Default Parent Path** and leave **Parent Field Name** blank.
- User-selected: your organization assigns loss events to a business entity that the user selects, for example, the Primary Caused Entity or the Primary Impacted Entity. To use this method, you enter the field name that contains the business entity in **Parent Field Name**. The field must be in the creation view.
- Pre-filled in a URL: your organization assigns loss events to a business entity that you pass in the URL. To use this method, you enter the field name that contains the business entity in **Parent Field Name**. Pass the value that you want in the URL.
- Custom: your organization sets the business entity based on information in the loss event or elsewhere in the system. For example, the system can automatically assign a loss event to Business Entity A if the loss amount is less than \$1,000,000 and to Business Entity B if it is over that amount. This method can be implemented with triggers. To use this method, you can leave **Parent Field Name** blank because it is set by the triggers.

The **Default Parent Path** is mandatory for all methods. The system defaults to it if the value in **Parent Field Name** is not given, is invalid, or there is an error. Ensure that the dedicated users have access rights to create loss events under the business entity in **Default Parent Path**.

## Who loss events get assigned to

---

Loss events are typically assigned to a triage team that is responsible for reviewing the initial information and taking next steps. You determine how this assignment is made when you define **Default Triage Team** and **Triage Team Field Name** in the **Loss Event Entry App** page.

For information, see [“Configuring the Loss Event Entry app” on page 839](#).

You can choose one of the following methods:

- Static: your organization assigns all loss events to a list of users and user groups. To use this method, you enter the list of users and user groups in **Default Triage Team** and leave **Triage Team Field Name** blank.
- User-selected: your organization assigns loss events to users or user groups that the user selects. To use this method, you put the field name that contains the actor field in **Triage Team Field Name**. The actor field must be in the Loss Events creation view.

**Note:** The default creation view for Loss Events (SysView-New-LossEvent-LEE) does not contain any actor fields. If you are using the default view, the **Triage Team Field Name** list is empty. To populate **Triage Team Field Name**, you need a custom creation view for Loss Events. In the custom view, add the actor field, such as Owner, that contains the users and groups you want to use for the triage team. If you add multiple actor fields, they must have the same display type. For more information, see [“Designing the loss entry form for the Loss Event Entry app” on page 833](#).

- Pre-filled in a URL: your organization assigns loss events to users or user groups that you pass in the URL. To use this method, you put the field name that contains the actor field in **Triage Team Field Name**.
- Custom: your organization assigns loss events to user or user groups based on information in the loss event or elsewhere in the system. For example, a trigger can take the value of a loss event's Primary Impacted Entity field and go to that entity's Preference record to get the name of the triage team. It can then put that triage team name into the triage team field on the loss event. To use this method, you can leave **Triage Team Field Name** blank because it is set by the triggers.

The **Default Triage Team** is mandatory for all methods. The system defaults to it if the value in **Triage Team Field Name** is not given, is invalid, or there is an error. Ensure that the field given in **Triage Team Field Name** is one of the six actor display types. If you pre-fill it in a URL, ensure that the values passed in the URL are consistent with the actor display types you chose in the **Triage Team Field Name**.

A third field, **Populate Triage Team Field Name**, is typically used as the assignee in workflows and configurable lifecycles for loss events. It is a mandatory field. When a loss event is created, the users

and user groups in **Triage Team Field Name** are copied to the field given in **Populate Triage Team Field Name**. If **Triage Team Field Name** is not given, the users and user groups in **Default Triage Team** are copied to the field given in **Populate Triage Team Field Name**. All three field types must be compatible. The display type of the field that is given in **Populate Triage Team Field Name** must be able to accept any value that comes from **Default Triage Team** or **Triage Team Field Name**. For example, if **Triage Team Field Name** is a multiple user/group field, **Populate Triage Team Field Name** must also be a multiple user/group field.

## How dates are validated

You define how dates are validated in rules in the **Date Validation** field in the **Loss Event Entry App** page. For example, you might want to ensure that a loss event's discovery date falls after its occurrence date and that the discovery date occurs before today's date.

The following date validation rules test for these situations:

LossEvent:Discovery Date	x ▾	on or before	x ▾	LossEvent:Recognition Date	x ▾
LossEvent:Discovery Date	x ▾	on or before	x ▾	TODAY	x ▾

Figure 82. Examples of date validation rules

OpenPages Loss Event Entry displays a red X and an explanation next to dates that fail the validation rules. Users must resolve errors before they can submit a loss event.

OpenPages Loss Event Entry includes date validation rules that you can keep or modify. The date validation rules are effective only in OpenPages Loss Event Entry and not in OpenPages. If you want the same validation rules to apply in OpenPages, you can implement them in the views. For more information, see “[Configuring rules](#)” on page 318.

## How to launch OpenPages Loss Event Entry

Users typically access IBM OpenPages Loss Event Entry from one or more links on your organization's intranet.

There are many ways that you can configure the URLs in these links:

- You do not pass parameters in the URL. Use this approach if you want users to provide information for loss events and you do not want to pre-fill information for them.
- You can set what locales users access. If all users access one locale, you can add the locale to the URL in the link on your organization's intranet. If users can access multiple locales, you can either place multiple links on your organizations intranet, for example, a link for users in North America and a link for users in France, or you can have one link and pre-fill the locale in the URL.
- You can pre-fill user information on the loss event form by passing fields and values in the URL. You can include user data from the network login and determine programmatically how to put it in the URL. When a user creates a loss event, values from the URL can pre-fill fields on the form. For example, the user's name, phone number, and email can be passed in the URL so that the user does not need to enter this information.
- You can pre-fill where in the organizational structure the loss event will be created and who it will be assigned to. Use this approach if your organization is structured in a way that loss events can be created in and assigned to multiple areas of the organization. You can use multiple URLs to pre-fill the primary caused business entity and the triage team. Then, users who create loss events do not need to enter this information, it is pre-filled for them and set to the correct value for where they are in the organization.
- You can pre-fill no information so that users can create loss events anonymously. Create a link where you do not pass user information. You must also ensure that users are not required to provide their name and email on the loss event form.

Follow these guidelines when you construct a URL:

- The fields that you pass must be defined for the top-level Loss Event object type.
- The fields that you pass must exist in the creation view.
- The fields that you pass cannot be read-only.
- The fields that you pass must be defined as one of the following data types: **Business Entity Selector**, **Simple String**, or **User/Group**. For more information, see “[Data types](#)” on page 155.

The following display types are supported: Business Entity Selector, Text, Text Area, Link, Group Selector, Multi Valued Group Selector, Multi Valued User Selector. Multi Valued User/Group Selector, User Selector, User/Group Selector, User Dropdown (legacy). All other display types are not supported.

- The values that you pass must be valid for the display type.
- The URL is limited to 2083 characters for Microsoft browsers.

Follow these syntax rules when you construct a URL:

- Start the first parameter with ?.
- Separate multiple parameters with &.
- Provide locales in the format `locale=<locale code>`. Valid locale codes are:
  - en\_US (US English)
  - en\_GB (UK English)
  - it\_IT (Italian)
  - pt\_BR (Brazilian Portuguese)
  - fr\_FR (French)
  - es\_ES (Spanish)
  - de\_DE (German)
  - zh\_TW (Chinese Traditional)
  - zh\_CN (Chinese Simplified)
  - ja\_JP (Japanese)
- Provide fields and values in the format `<field group>:<field name>=<field value>`. Enter the field name not the field label.
- For fields whose display type is Multi-Valued User Selector, Multi-Valued Group Selector, or Multi-Valued User/Group Selector, you can pre-fill the field with one or multiple values. Begin and end values with \$;, for example:

```
$;user1$;
```

Use \$; to separate multiple values. For example:

```
$;user1$;user2$;user3$;
```

- For text fields that pass email addresses, for example, **Submitter Email Field Name**, you can pre-fill the field with only one value.

The following examples illustrate how you can construct URLs.

Example 1: Set the locale.

```
http://<server>:<port>/openpages/app/jspview/appLoader/lossevent?locale=en_GB
```

Example 2: Pre-fill the primary caused entity to /Global Services/North America Banking. The display type of OPSS-LE-BE:Primary Caused Entity is business entity selector.

```
http://<server>:<port>/openpages/app/jspview/appLoader/lossevent
?OPSS-LE-BE:Primary Caused Entity=/Global Services/North America Banking
```

Example 3: Pre-fill the triage team to Risk Team New York and two users:

```
http://<server>:<port>/openpages/app/jspview/appLoader/lossevent
?ABC-LE:UsersToNotify=$;Risk Team New York$;user1$;user2$;
```

Example 4: Pre-fill user information from the network sign-on:

```
http://<server>:<port>/openpages/app/jspview/appLoader/lossevent
?OPSS-LE-Contact:Your Name=User One&OPSS-LE-Contact:Your Email=user1@example.com
```

Example 5: Pre-fill user information, primary caused business entity, and locale:

```
http://<server>:<port>/openpages/app/jspview/appLoader/lossevent
?OPSS-LE-Contact:Your Name=User One&OPSS-LE-Contact:Your Email=user1@example.com
&OPSS-LE-Contact:Your Phone=555-111-2222&OPSS-LE-BE:Primary Caused Entity=
/Global Services/North America Banking&locale=en_GB
```

Example 6: Pre-fill information if you have multiple primary caused business entities and multiple triage teams in your organization. Assume that you have two divisions, /Global Services/North America/Division/East and /Global Services/North America/Division/West. You want to prefill the parent business entity with the division's Primary Caused Entity and the triage teams from ABC-LE:UsersToNotify.

You create two URLs. This URL is for users in the East division.

```
http://<server>:<port>/openpages/app/jspview/appLoader/lossevent
?OPSS-LE-BE:Primary Caused Entity=/Global Services/North America/Division/East
&ABC-LE:UsersToNotify=DivisionEastTriage
```

This URL is for users in the West division.

```
http://<server>:<port>/openpages/app/jspview/appLoader/lossevent
?OPSS-LE-BE:Primary Caused Entity=/Global Services/North America/Division/West
&ABC-LE:UsersToNotify=DivisionWestTriage
```

Example 7: Pre-fill no information for a URL that you use for loss events that are created anonymously. Do not pass user information. You might want to send the email confirmation to a person designated to handle these situations.

```
http://<server>:<port>/openpages/app/jspview/appLoader/lossevent
?LE-Submitter:Confirmation Emails=user5@example.com
```

**Note:** You cannot use IBM OpenPages Loss Event Entry and IBM OpenPages with Watson at the same time. To return to OpenPages, close the IBM OpenPages Loss Event Entry browser window, open a new browser window, and then log in to OpenPages.

## How confirmation emails are configured

You can design and configure the confirmation email that is sent to users when a loss event is created.

The confirmation email has the following parts:

- Submitter email address

In the **Loss Event Entry App** page, click **Submitter Email Field Name** and select a field. Email confirmations are sent to the value of this field. The default is OPSS-LE-Contact:Your Email.

- Text and parameters to put in the subject

In the **Loss Event Entry App** page, click **Submitter Email Subject Parameters** and select the fields that you want to put in the email subject.

Next, write the text and enter parameters for those fields in  > **System Configuration > Application Text > lossevent.confirm.subject**. The order of the fields that are listed in **Submitter Email Subject Parameters** must match the numbering of the parameters in lossevent.confirm.subject.

- Text and parameters to put in the body text

In the **Loss Event Entry App** page, click **Submitter Email Body Parameters** and select the fields to include in the email body.

Next, write the text and enter parameters for those fields in > **System Configuration > Application Text > lossevent.confirm.content**. The order of the fields that are listed in **Submitter Email Body Parameters** must match the numbering of the parameters in **lossevent.confirm.content**.

- Sender email address

Enter the system email address that sends confirmation emails in > **System Configuration > Application Text > lossevent.confirm.from.address**. Parameters are not allowed in **lossevent.confirm.from.address**.

Use the following syntax in **lossevent.confirm.subject**:

- Enter **{0}** for the first parameter, which in the out-of-the box configuration is the name of the loss event. Enter additional parameters in the syntax **{value}**. The values of fields given in **Submitter Email Subject Parameters** are put in the email subject.

Use the following syntax in **lossevent.confirm.content**:

- Enter **{1}** for the first parameter, which in the out-of-the box configuration is the name of the submitter. Enter additional parameters in the syntax **{label}:{value}** or **{value}**.

For example, **{2}:{3}** puts the label and value of the second field given in **Submitter Email Body Parameters** in the email body. Then, **{4}:{5}** puts the third field, **{6}:{7}** the fourth field, and so on.

For example, **{2}:{3} \n {4}:{5}** puts the second field's label and value, a line break, and the third field's label and value in the body text.

Enter **{value}** to omit a field label. For example, **{3} \n {5}** puts the second field's value, a line break, and the third field's value in the body text (without the field labels).

- Use **\$children** to include loss event impacts and loss recoveries in the email.
- Use **\$title** to include the label of the loss event object type in the email.
- Enter **\n** to force a line break.

For example, if **Submitter Email Body Parameters** is defined as:

```
OPSS-LE-Contact:Your Name
OPSS-LossEv:Owner
System Fields:Name
System Fields:Description
OPSS-LE-BE:Primary Caused Entity
```

And the **lossevent.confirm.content** application text string is defined as:

```
{1}, \nThe following $title was entered by you. \n{2}: {3} \n{4}: {5} \n{6}: {7}\n \n
{8}: {9}
\n\nDo not reply. Automated email from OpenPages
```

The confirmation email contains the following body text:

```
User One,
The following Loss Event was entered by you.
Owner: Administrator
Name: Library_LE_0022
Description: This is a description
Primary Caused Entity: /Global Services/North America

Do not reply. Automated email from OpenPages
```

The value for **OPSS-LE-Contact:Your Name** is substituted into parameter **{1}** followed by a line break, text, and another line break.

The label and value for **OPSS-LossEv:Owner** is substituted into parameters **{2}: {3}** followed by a line break.

The label and value for System Fields:Name is substituted into parameters {4}: {5} followed by a line break.

The label and value for System Fields:Description is substituted into parameters {6}: {7} followed by a line break.

The label and value OPSS-LE-BE:Primary Caused Entity is substituted into parameters {8}: {9} followed by a line break.

The ending text is included.

## Configuring the Loss Event Entry app

---

You use the **Loss Event Entry App** page to configure IBM OpenPages Loss Event Entry.

### Before you begin

To do this task, you need the following access permissions:

- You must be a member of the OPAdministrators group.
- You must have Write access to the **System Files > End User Applications Config** folder.
- You must use a profile that has access to all of the following object types: Loss Event, Loss Impact, Loss Recovery, and File (SOXDocument).

Read [Chapter 32, “Configuring OpenPages Loss Event Entry,” on page 831](#) to learn about OpenPages Loss Event Entry and [“Planning the configuration ” on page 831](#) to learn about decisions to make before you begin.

### Procedure

1. Click  > **Integrations > Loss Event Entry App**.
2. Complete the fields in the **Other** section.
  - a) In **Default Parent Path**, select the default parent business entity for new loss events.  
This business entity is used if users cannot or do not select a parent business entity when they enter a loss event.
  - b) In **Parent Field Name**, select the field that contains the business entities that users can choose from when they set the parent for a new loss event.  
The list displays Business Entity Selector fields that are included in the Loss Events creation view. The default is OPSS-LE-BE:Primary Caused Entity.  
If not given or the user does not select a value in this field, the value in **Default Parent Path** is used as the parent for a loss event.
  - c) In **Submitter Email Field Name**, select the field that contains the email to which confirmations will be sent.  
The list displays fields that are defined in the creation view for Loss Events and have a Text Box display type. The default is OPSS-LE-Contact:Your Email.
  - d) In **Populate Triage Team Field Name**, select the field that will store the name of the triage team for loss events.  
For more information, see [“Who loss events get assigned to ” on page 834](#).  
The default is OPSS-LossEv:Owner.
  - e) Optional: Depending on your configuration, you might be able to choose a value in the **Triage Team Field Name** field. Select the field that contains the name of the assignee for new loss events. New loss events are assigned to the value of this field.  
If **Triage Team Field Name** is empty, continue to the next step.

**Note:** If the **Triage Team Field Name** list is empty, check the creation view for Loss Events. The **Triage Team Field Name** list displays user and group fields that are defined in the Loss Events creation view.

If **Triage Team Field Name** is blank and the user does not select a value for this field in the app, the value in **Default Triage Team** is used for the assignee.

- f) In **Default Triage Team**, select the users and groups that loss events are assigned to for follow up. The value of **Default Triage Team** is used when a triage team isn't specified elsewhere.
- g) Select **Display Resource ID of Created Objects** to show a loss event's internal system-generated identifier to the user on the confirmation page and in the confirmation email.
- h) Review the **Date Validation** rules and make changes, if needed.

Follow these guidelines:

- You can use only date fields, and they must exist in the object's creation view.
- You can use date fields on the Loss Event object or any of the other object types that are used by OpenPages Loss Event Entry. A rule cannot cross object types.
- You can use TODAY to validate against the current date.

- i) In **Submitter Email Subject Parameters**, select the fields to include in the subject of the confirmation email that is sent to the submitter. The default is System Fields:Name.

You can choose any of the fields in the Loss Event profile. The Application Text that is located in lossevent.confirm.subject references these parameters.

For more information, see [“How confirmation emails are configured” on page 837](#).

- j) In **Submitter Email Body Parameters**, select the fields to include in the body of the confirmation email that is sent to the submitter. The default is OPSS-LE-Contact:Your Name, System Fields:Name, System Fields:Resource ID, System Fields:Description.

You can choose any of the fields in the Loss Event profile. The Application Text that is located in lossevent.confirm.content references these parameters.

For more information, see [“How confirmation emails are configured” on page 837](#).

3. If you want to configure the tabs that users see in the Loss Event Entry app, click the **Content** section and do the following steps:

- a) If you want to hide tabs for the object types that are related to the Loss Event object type, click **Additional Object Types** and deselect them.

For example, if you want to hide the **Loss Recoveries** tab, deselect **Loss Recoveries**.

- b) If you want a tab to be mandatory, click **Required** and select it from the list.

This example shows what the app looks like for users when the **Loss Recoveries** tab is hidden and the **Loss Impacts** tab is **Required**.

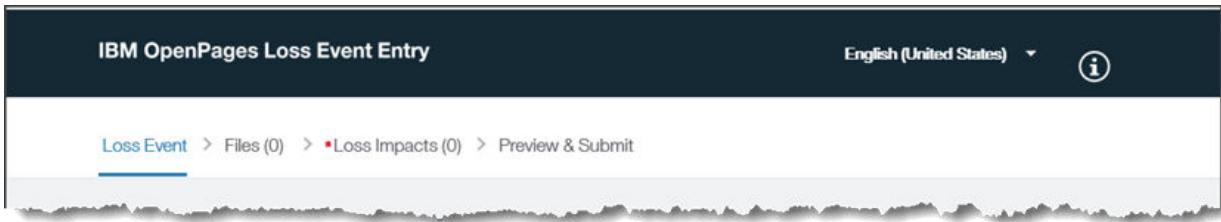


Figure 83. Tabs in Loss Event Entry

4. If you want to configure locales for Loss Event Entry, click the **Locales** section and do the following steps:

- a) Select a **Default Locale**. This locale is used when a locale is not specified in the URL that launches Loss Event Entry.

The locale determines the language and the currency, date, and number format that users see. If you configure additional locales, users can switch between locales and the default locale.

b) To use more locales, click **Enabled**, and then enter a password for the dedicated locale user.

For more information, see “[How users are handled](#)” on page 833.

You must enter a password for each locale that you enable.

To change the dedicated users' passwords in the future, always use  > **Integrations > Loss Event Entry App** rather than  > **Users and Security > Users**.

**Important:** Do not change the dedicated users' passwords by using  > **Users and Security > Users**. Otherwise, users will not be able to use Loss Event Entry because the passwords will be out of sync.

You can use the usernames that are provided by default or you can change them. If you change the usernames in the **Loss Event Entry App** page, they must match the usernames of the dedicated users that you create with  > **Users and Security > Users**.

For each dedicated user, ensure that the **User cannot change password** and **Password never expires** options are enabled. To view these settings, go to  > **Users and Security > Users**, select a dedicated user, and then click **Reset password**.

5. Click **Submit**.

If the **Submit** button is not enabled, click **Why can't I save** to find out which fields you need to complete.



# Chapter 33. Configuring IBM Watson Integrations

OpenPages can be integrated with IBM Watson Assistant, IBM Watson Language Translator, and a natural language processing service.

## IBM Watson Assistant

Configure an assistant and integrate it with OpenPages so that users can ask free-format questions and receive answers using a chat bot.

IBM Watson Assistant is a chat bot that can appear in the UI. It can offer 24-hour support to the common questions that users have within OpenPages. It can provide interactive text answers, natural language search, and direct links to specific pages in OpenPages, for example, to a Creation View where a user can enter an Issue or Loss Event. A subscription to the IBM Watson Assistant service is required.

When an assistant is configured, the **Start Chat**  icon is displayed on all pages in the UI. It is displayed only to users with the application permission that allows them to access it.

### Configuration overview

Complete the following steps to configure IBM Watson Assistant:

1. Configure an assistant. For more information, see “[Configuring a web chat assistant by using IBM Watson Assistant](#)” on page 843.
2. Integrate the assistant with OpenPages. For more information, see “[Configuring the integration between an assistant and OpenPages](#)” on page 844.

### Show me how

This video provides an overview of using IBM Watson Assistant.

<https://youtu.be/NbvU-UdJ6Aw>

## Configuring a web chat assistant by using IBM Watson Assistant

An assistant must be configured before it can be integrated with OpenPages.

### Before you begin

Learn about IBM Watson Assistant using the extensive documentation, tutorials, and videos that IBM provides. For more information, see the [IBM Cloud® documentation](#).

Choose a subscription for IBM Watson Assistant that includes the web chat interface. For example, the Assistant Plus subscription includes the web chat interface.

### About this task

An assistant is a cognitive bot to which you add skills that enable it to interact with your users in useful ways.

The assistant must be saved with a web chat integration.

**Note:** You can create an assistant on IBM Cloud Pak for Data or on IBM Cloud.

### Procedure

1. Create an assistant and configure skills that match the needs of OpenPages users.

## 2. Add a web chat integration to the assistant.

When you add a web chat integration, a code snippet is displayed in the **Add the chat UI to your web page** section. You need parts of the code snippet to integrate the assistant with OpenPages.

## 3. In **Customize your chat UI**, you can optionally change the style of the assistant. If you add an avatar image, make a note of the image URL because it must also be added in the OpenPages integration.

### What to do next

Integrate the assistant with OpenPages. For more information, see “[Configuring the integration between an assistant and OpenPages](#)” on page 844.

Configuring IBM Watson Assistant is an iterative process. As users work with it, you can improve and expand the skills. You might need to change or expand the skills as they change over time. You can also download a skills data usage report and improve it.

## Configuring the integration between an assistant and OpenPages

Add integration information for an assistant so that it displays in the UI in OpenPages.

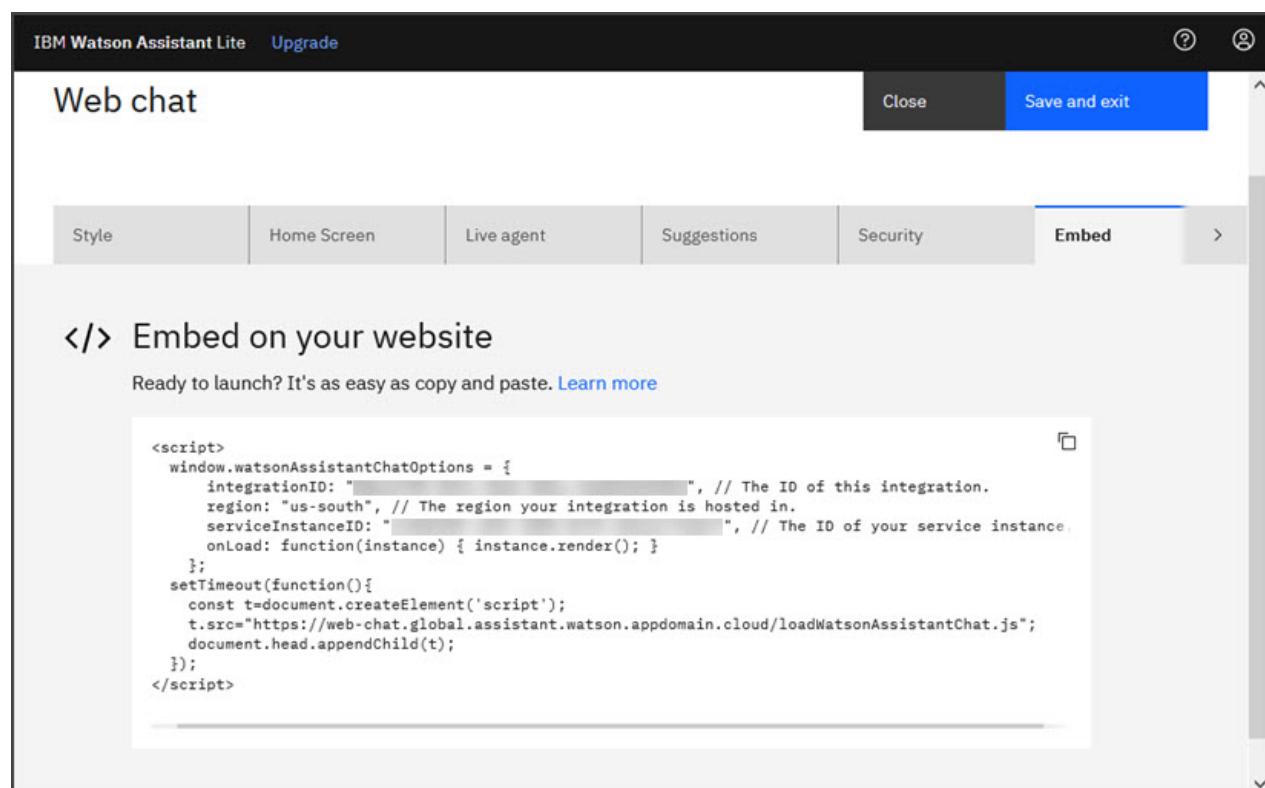
### Before you begin

Add the **SOX > Administration > User Interfaces > Watson Assistant UI** application permission to role templates that are allowed to access IBM Watson Assistant .

Configure an assistant. For more information, see “[Configuring a web chat assistant by using IBM Watson Assistant](#)” on page 843.

### About this task

When an assistant is configured and saved with a web chat integration, a code snippet is displayed in the **Embed** section. You can import the code into the **Watson Assistant** page in OpenPages.



The screenshot shows the IBM Watson Assistant Lite interface. At the top, there's a navigation bar with 'IBM Watson Assistant Lite' and 'Upgrade' buttons. Below the navigation bar, the title 'Web chat' is displayed. On the right side of the screen, there are two buttons: 'Close' and 'Save and exit'. A horizontal tab bar below the title includes tabs for 'Style', 'Home Screen', 'Live agent', 'Suggestions', 'Security', and 'Embed'. The 'Embed' tab is currently selected and highlighted in blue. Below the tabs, the text '</> Embed on your website' is shown. Underneath this text, there's a message 'Ready to launch? It's as easy as copy and paste.' followed by a link 'Learn more'. A large text area contains a script tag with code for embedding the chat. The code includes variables like 'integrationID', 'region', 'serviceInstanceID', and 'onLoad'.

```
<script>
window.watsonAssistantChatOptions = {
 integrationID: "REDACTED", // The ID of this integration.
 region: "us-south", // The region your integration is hosted in.
 serviceInstanceID: "REDACTED", // The ID of your service instance.
 onLoad: function(instance) { instance.render(); }
};
setTimeout(function(){
 const t=document.createElement('script');
 t.src="https://web-chat.global.assistant.watson.appdomain.cloud/loadWatsonAssistantChat.js";
 document.head.appendChild(t);
});
</script>
```

## Procedure

1. Open the code snippet that is displayed when an assistant is saved with a web chat integration.
2. Click  > **Integrations** > **Watson Assistant**.
3. Click .
4. Paste the code snippet into the **Configuration string** box, and then click **Import**.  
The **Web Chat Options** table displays the values for your web chat assistant.
5. If the assistant is defined with an avatar image, enter the URL in **Assistant Image URLs**.
6. In **Assistant Profiles**, select the profiles that are allowed to access IBM Watson Assistant .
7. Click **Save**.
8. If you are using IBM Cloud Pak for Data, add your web chat URL to the list of allowed URLs in OpenPages.
  - a) In the **Web Chat Options** table, click **cloudPrivateHostURL** and copy its value.
  - b) Click  > **System Configuration** > **Settings**.
  - c) Click the **Applications** > **Assistant** > **Embedded Assistant URLs**
  - d) In the **Value** field, add the URL that you copied in step “8.a” on page 845 to the list of URLs.
  - e) Click **Done**.

## What to do next

Refresh the screen and test the assistant within OpenPages. Refine it as needed.

**Tip:** If the configuration of your assistant changes, you can re-import its code snippet. Or, you can edit the values in the **Web Chat Options** table.

## Enabling additional security features for IBM Watson Assistant on IBM Cloud

IBM Watson Assistant has features around making sure that chat conversations are coming to IBM Watson Assistant from your web chat in an authorized way. You can turn on these additional security features for your web chat assistant. This task is optional.

### About this task

For more information, see [Security](#) in the IBM Watson Assistant documentation.

## Procedure

1. Generate RS256 2048-bit public and private keys.  
For example, you can use OpenSSL to create the keys:

```
openssl genrsa -out private.pem 2048
openssl rsa -in private.pem -pubout -out public.pem
```

Save the keys. You need them in a later step.

2. Go to the configuration page for your web chat assistant on IBM Cloud or IBM Cloud Pak for Data.
3. Click the **Security** tab, and enable web chat security.

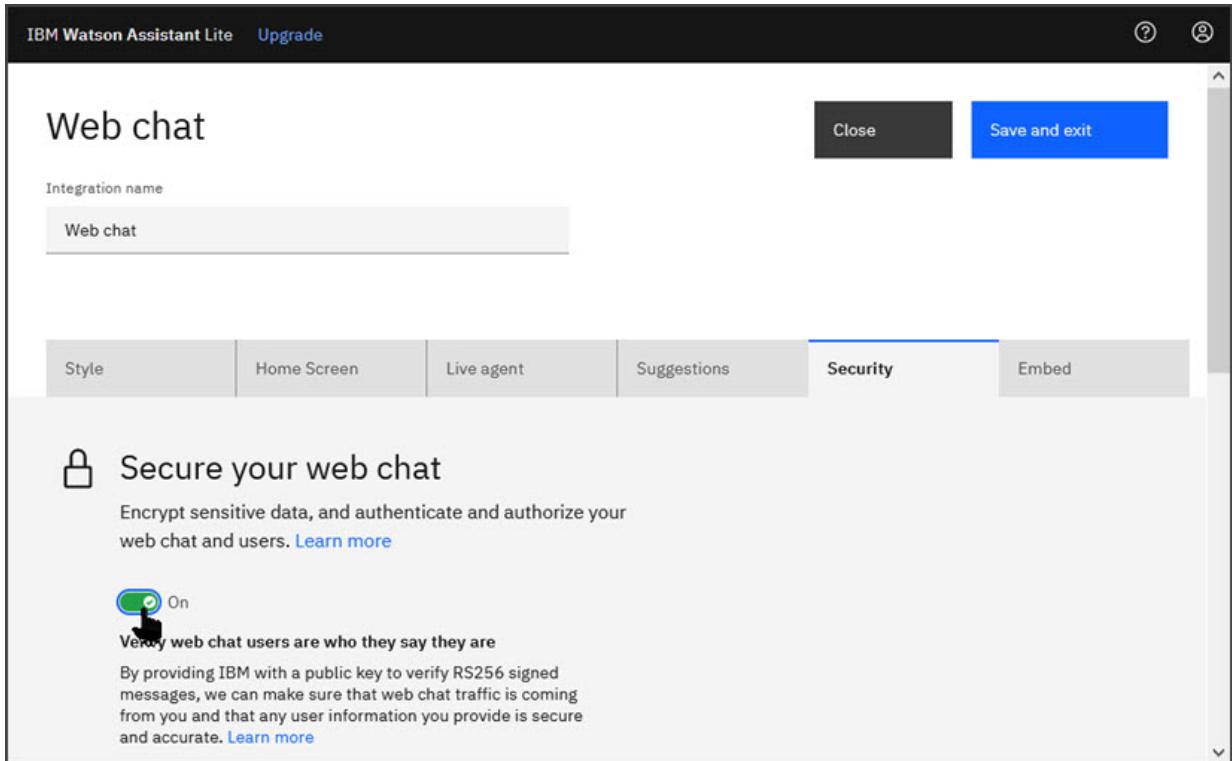


Figure 84. Enabling web chat security in IBM Watson Assistant

4. In the **Your public key** field, paste the public key that you created in step 1.

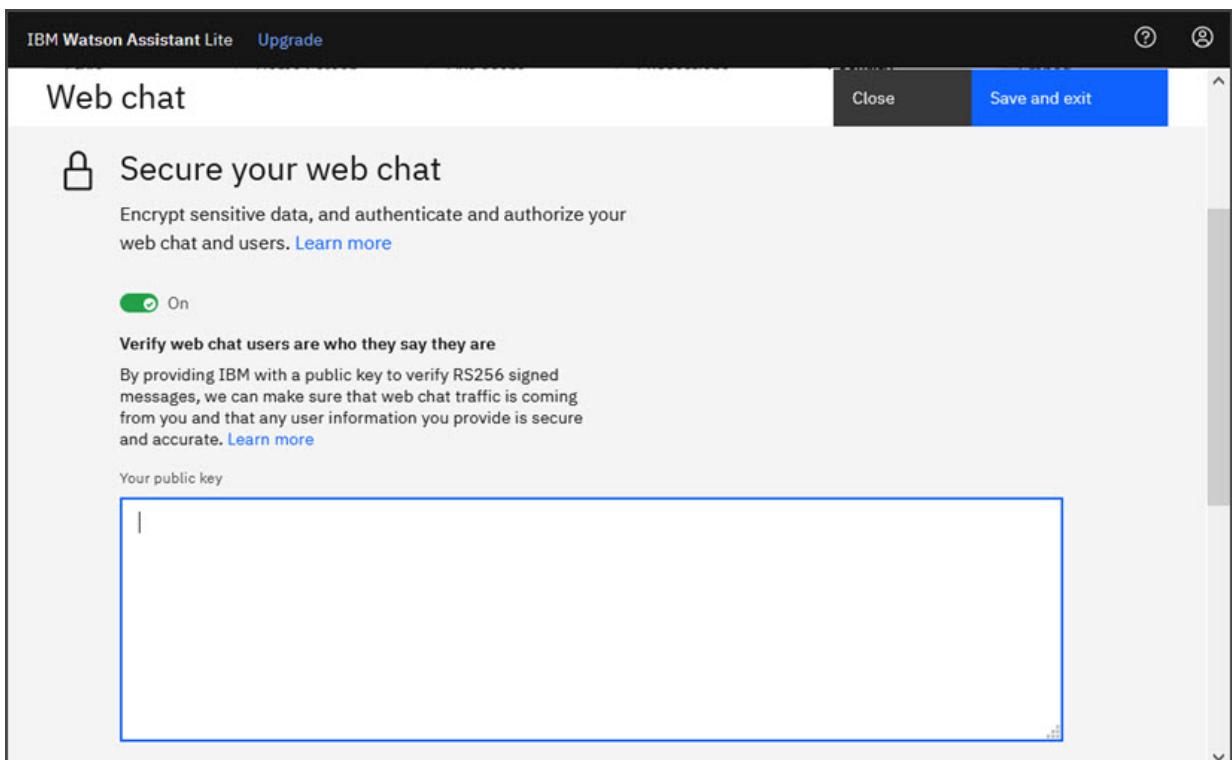


Figure 85. Adding your public key to your web chat assistant

5. Log in to OpenPages as a user with the **Watson Assistant** application permission.
6. Click > **Integrations** > **Watson Assistant**.
7. In the **Private Key** field, paste the private key that you created in step 1.

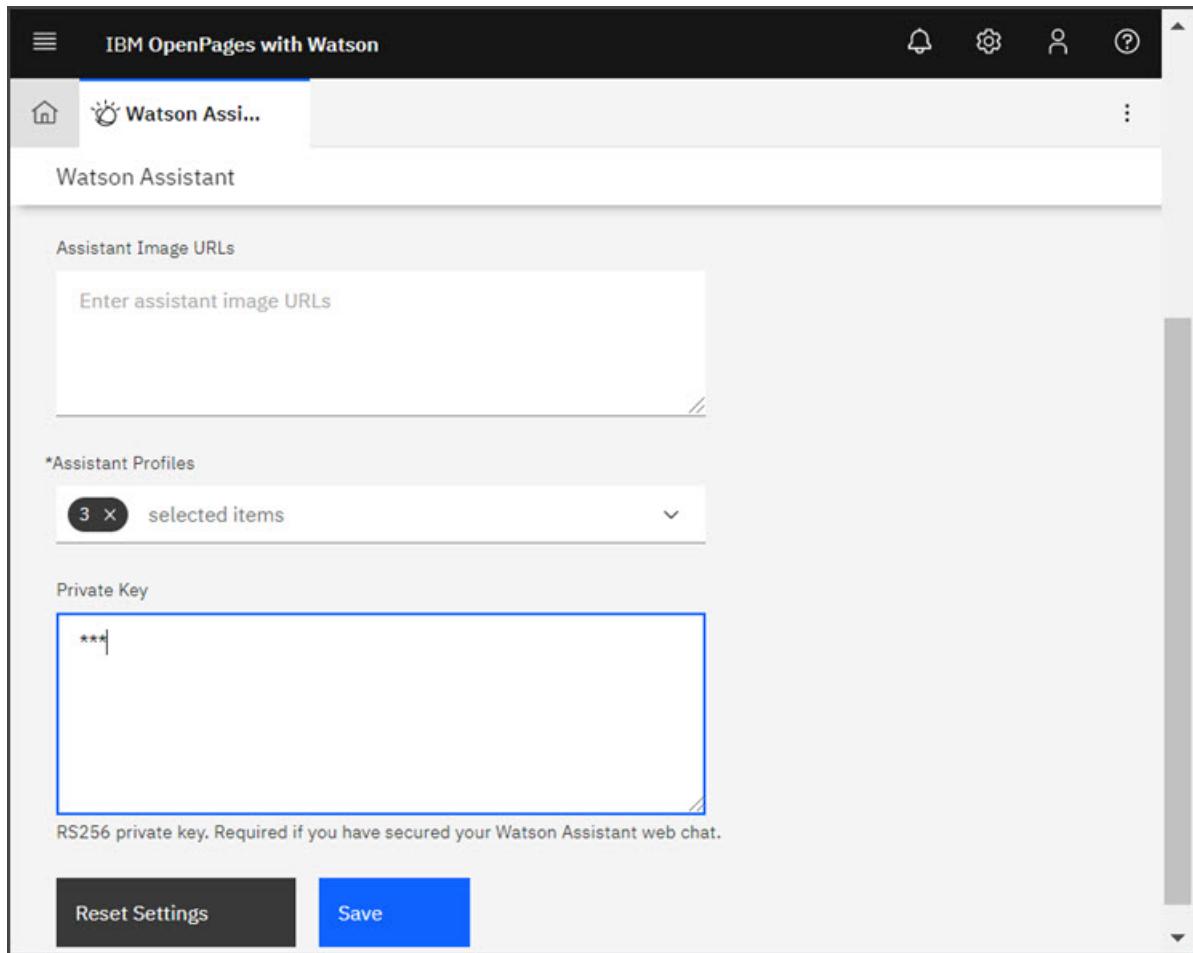


Figure 86. Adding your private key in OpenPages

8. Click **Save**.

## IBM Watson Language Translator

Configure IBM Watson Language Translator so that users and administrators can translate text as they work.

The icons and functionality for the IBM Watson Language Translator are different depending on whether the access point is for users or administrators.

### How users interact with IBM Watson Language Translator

Users can work with translated text by using the and icons in Task Views.

In a Task View, a user can click . Values in text fields are translated to the language associated to their locale. For each field that is translated, the user can toggle between the languages by clicking **View Original** and **View Translation**. Click the Info icon to view a confidence score.

Click to turn off translated values.

- Text field values (simple strings and long strings) are translated. Rich text fields and enumerated field values are not translated.
- There is no differentiation between US and UK English.

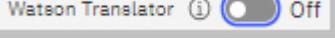
- Translated values on a Task View cannot be edited.
- They are not saved to the object.

Example 1: a user's locale is set to US English. The user views regulatory change objects in a Task View.

- First, the user views a regulatory change object that came from a French regulatory body. It contains

field values in French. The user clicks the  icon. Text field values in French are translated to English.

- Next, the user views a regulatory change object that came from an EU regulatory body. It contains text

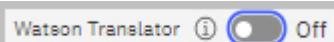
field values in English, French, and Portuguese. The user clicks the  icon. The text field values in English remain unchanged. The text field values in French and Portuguese are translated into English.

Example 2: a user's locale is set to Japanese. The user views regulatory change objects in a Task View.

- First, the user views a regulatory change object that came from a US regulatory body. It contains field

values in English. The user clicks the  icon. Text field values in English are translated into Japanese.

- Next, the user views a regulatory change object that came from an EU regulatory body. It contains field

values in English, French, and Portuguese. The user clicks the  icon. Text field values are translated into Japanese.

## How administrators interact with IBM Watson Language Translator

Administrators can work with translated text by using the  icon on the following screens:

- Application Text
- Object Text
- Fields
- Dashboard configuration (administrators)
- View Designer
- GRC Workflow Designer

The  icon is available on screens where labels in multiple languages are defined. The original field value is translated into other languages. Translated values can be edited and they are saved.

Example 1: an administrator's locale is set to U.S. English. The administrator creates a new workflow using the GRC Workflow Designer.

- When defining stages in the workflow, the administrator enters a label in English and clicks **Edit**. Initially, the English text is displayed as label values for the other languages. The administrator clicks

 and translated values are populated to the other languages. The administrator clicks **Done** to save the stage.

Example 2: an administrator's locale is set to Simplified Chinese. The administrator creates views using the View Designer.

- When defining elements in the view, the administrator enters a text value in Simplified Chinese and clicks **Edit**. Initially, the Simplified Chinese text is displayed as label values for the other languages. The

administrator clicks  and translated values are populated to the other languages. The administrator clicks **Done** to save the values.

## Configuration overview

Complete the following steps to configure IBM Watson Language Translator:

1. Configure IBM Watson Language Translator on IBM Cloud. For more information, see “[Configuring IBM Watson Language Translator on IBM Cloud](#)” on page 849.
2. Configure the integration between IBM Watson Language Translator and OpenPages. For more information, see “[Configuring the integration between IBM Watson Language Translator and OpenPages](#)” on page 849.

## Configuring IBM Watson Language Translator on IBM Cloud

An IBM Watson Language Translator service must be configured before it can be integrated with OpenPages.

### Before you begin

Learn about IBM Watson Language Translator using the extensive documentation, tutorials, and videos that IBM provides. For more information, see the [IBM Cloud documentation](#).

You can choose any pricing plan. If you have specific translation requirements, for example, complex legal texts, you may want to choose a plan that you can train.

### Procedure

1. Create an IBM Cloud account if one does not already exist.
2. Log in, create the service, and get your service URL and API key. You need them later when you configure IBM Watson Language Translator in OpenPages.  
After you create an instance of the IBM Watson Language Translator service, you can view the service URL and API key by going to the service dashboard, finding the service, and clicking **Manage** and **Show Credentials**.
3. Depending on the pricing plan you chose, you might be able to train the IBM Watson Language Translator service.

### What to do next

Complete the remaining tasks that are described in “[IBM Watson Language Translator](#)” on page 847.

## Configuring the integration between IBM Watson Language Translator and OpenPages

Define integration information for IBM Watson Language Translator so that it can be used in the UI in OpenPages.

### Before you begin

You need a IBM Watson Language Translator service. For more information, see “[Configuring IBM Watson Language Translator on IBM Cloud](#)” on page 849.

Set the following application permissions:

- Set the **Watson Language Translator** permissions for administrators who are allowed to access the  > **Integrations** > **Watson Language Translator** menu item.
- Set the **Watson Language Translator UI** permission for users who are allowed to use IBM Watson

Language Translator to view translated text in Task Views by using the 

icon. It also allows access to the  icon from administrator tasks.

For more information, see “[Types of application permissions](#)” on page 52.

## Procedure

1. Get the service URL and API key for the IBM Watson Language Translator service. For more information, see “[Configuring IBM Watson Language Translator on IBM Cloud](#)” on page 849.
2. Click  > **Integrations** > **Watson Language Translator**.
3. Copy the IBM Watson Language Translator service URL into **Service URL**.
4. Optional: Type the IBM Watson Language Translator API version into **API Version**.  
To use the default value that is used by OpenPages, leave the field empty.  
For more information, see [Versioning](#) in the IBM Watson Language Translator documentation.
5. Copy the IBM Watson Language Translator API key into **API Key**.
6. In **Confidence Threshold** enter the lowest confidence score that a suggestion must meet. This is a confidence score for recognizing a particular language. It is not a confidence score of the quality of the translated text.
7. Define the object types that are allowed to be translated.
  - To enable translation for all object types, set **Enable all Object Types** to true.
  - To restrict translation to specific object types, set **Enable all Object Types** to false. Under **Object Types**, click the check box next to each object type that is allowed to be translated.
8. Click **Save**.
9. Click **Test Connection** to check the connection.
10. Test the functionality across the system.  
You can use the following logging options to help you to troubleshoot the integration:
  - You can enable trace logging to collect debug information. See “[Gathering logs with the LogCollector user interface](#)” on page 693.
  - You can use **Applications** > **Watson Language Translator** > **Watson SDK Logging** to set the logging level for HTTP requests from OpenPages to IBM Watson Language Translator. This setting is used when trace logging is enabled. See “[Configure HTTP request logging for IBM Watson Language Translator](#)” on page 498.

## Results

**Note:** Should you ever want to turn off the IBM Watson Language Translator feature after it has been configured, clear the **Watson Language Translator UI** permission on users. The buttons for the IBM Watson Language Translator are then hidden.

## Natural language processing services

---

Configure a natural language processing service and integrate it with OpenPages so that users have support when they classify objects and make object associations. A natural language processing service understands the intent behind text and returns suggestions, together with a confidence score.

The following natural language processing services are supported:

- IBM Watson Discovery in IBM Cloud Pak for Data
- IBM Watson Natural Language Understanding in IBM Cloud

You can configure a natural language processing service to suggest either taxonomy classifications or parent and child object associations. You can use it for any objects in OpenPages but it is typically used to classify loss events, waivers, issues, and incidents or to associate them to a risk, policy, or control.

If you configure it to suggest taxonomy classifications, you can use it, for example, to support users when they classify a loss event to the correct Basel II categorization or when they classify waivers as exceptions

to regulatory compliance. The text description that a user enters is used as input to a natural language processing service that has been trained with knowledge from your domain specialists.

If you configure it to suggest object associations, you can use it to support users when they, for example, create an Issue object and need to associate it to a parent Control object. Again, the text description that a user enters is used as input to a natural language processing service but in this case it returns a suggested parent Control object together with a confidence score. Object association suggestions can be configured to suggest either parent or child associations. They are synchronized with associations that users make for parent or child objects.

Using a natural language processing service is best suited to situations where users are generating a high volume of objects, hundreds or even thousands per year. Cognitive computing adds value when it is scaled to a large data set and to a large group of users. The data the classifier is trained on should be relatively small and static. For example, you would want to train a classifier to provide object association suggestions to a small number of Controls in the Controls Library, which is small and relatively static, rather than to all the Controls in your business, which are numerous and dynamic. You would not want to train a classifier to make object associations between objects that change rapidly, for example, Audit Findings and Issues, because Issues are constantly changing and there might be thousands of them.

You can link OpenPages to one or more services, either to support different purposes or multiple languages.

## Terms to understand

### natural language processing service

A natural language processing service uses machine learning algorithms to return the top-matching predefined classes for short text inputs.

### IBM Watson Discovery

IBM Watson Discovery is a natural language processing service on IBM Cloud Pak for Data. You configure a IBM Watson Discovery service and then integrate it with OpenPages. It uses the Analyze API.

### IBM Watson Natural Language Understanding

IBM Watson Natural Language Understanding is a language processing service in IBM Cloud. You can train and deploy text classifier models and then integrate them with OpenPages. IBM Watson Natural Language Understanding learns from your data and can predict classifications for texts that it is not trained on. IBM Watson Natural Language Understanding is a multi-label, multi-class classifier. It assumes that text likely belongs to more than one class and can better predict texts with multiple classifications.

### Classifier Configuration

A classifier configuration in OpenPages defines connection information to an instance of a natural language processing service. For taxonomy classifications, it specifies the classifier target fields for the instance. For object associations, it specifies the object type to associate, whether it is a child or parent relationship, and other attributes.

### Classifier Field

A classifier field is a field group in OpenPages that contains the name of a classifier configuration and a classifier input field. An IBM Watson Insights button is displayed in place of a classifier field (taxonomy classifications) or as an action (object associations).

### Classifier Input Field

A classifier input field is a field in OpenPages that contains the short text input that a natural language processing service interprets and classifies. It is typically a **Description** field. The text *Adding a description improves IBM Watson Suggestions* is automatically displayed below a classifier input field.

### Classifier Target Fields

For taxonomy classifications, classifier target fields are fields in OpenPages that are set when a user chooses suggestions for a classifier field.

### Watson Insights

The underlying infrastructure in OpenPages is tied to IBM Watson Insights. An IBM Watson Insights button is displayed and suggestions are displayed in a **Watson Insights** panel.

An IBM Watson Insights button appears only if the classifier is able to make a suggestion based on the text entered. The button does not appear if the text does not generate suggestions.

The user interaction in the **Watson Insights** panel is the same regardless of whether the service is IBM Watson Discovery or IBM Watson Natural Language Understanding.

## Configuration overview for natural language classifier services

To use OpenPages together with a natural language processing service, you must design how you want the system to work and complete several configuration tasks.

### Before you begin

- Decide what type of service to use:
  - IBM Watson Discovery in IBM Cloud Pak for Data
  - IBM Watson Natural Language Understanding in IBM Cloud
- Decide the purpose of the classifier: taxonomy suggestions or object association suggestions.
- Verify that the application server has outgoing internet access so that it can communicate with classifier services.
- Verify that the data type for the classifier input field is Simple String.
- If the classifier is for taxonomy suggestions:
  - Decide what area you want to support, for example, helping users select Basel II categorizations.
  - Decide what objects the classifier field is available on, for example, loss events, waivers, issues, and incidents.
  - Verify that the data type for the classifier target fields is Enumerated String. You can have up to three classifier target fields.
  - Decide whether you want to allow users to select one or many suggestions. Set **Multi-valued** to false on at least one of the classifier target fields to allow users to select only one suggestion. Set **Multi-valued** to true on all classifier target fields to allow multiple selections.
- If the classifier is for object association suggestions:
  - Decide on the object types and associations that you want to use. For example, suppose you want to create a classifier that helps users to map issues to controls. In this case, you need the classifier to analyze the description of the issue objects, and then suggest parent controls for the issues.
  - Decide what objects the classifier field is available on. For example, if you're mapping issues to controls, the classifier field needs to be available on issues.
  - Verify the path to the object type that you want to associate to. For example, if you're mapping issues to controls, verify the path of the controls.
  - Decide what names and descriptions are displayed when a user selects an object.

### About this task

The following steps describe how to configure a natural language processing service.

### Procedure

1. Configure and train the natural language processing service.
  - IBM Watson Discovery. For more information, see [“Configuring Watson Discovery” on page 853](#).
  - IBM Watson Natural Language Understanding in IBM Cloud
2. Define a classifier configuration. For more information, see [“Defining a classifier configuration” on page 854](#).
3. Define a classifier field. For more information, see [“Defining a classifier field” on page 855](#).
4. If it is not already there, add the classifier field's field group to the object type.

5. Add the classifier field to the profile.
6. Add the classifier field to views where you want it to display. For more information, see “[Adding a classifier field that makes taxonomy suggestions](#)” on page 288 and “[Adding a classifier field that makes object association suggestions](#)” on page 309.
7. Re-create the reporting framework so you can access usage data in Cognos. Do this only one time, not for every service you configure. For more information, see “[Generating the reporting framework](#)” on page 814.
8. Test the configuration and resolve errors.

If you encounter connection issues with IBM Watson Discovery, import the Watson certificate into the WebSphere Liberty truststore. Do this only one time, not for every service you configure. For more information, see “[Importing a certificate for Watson services on IBM Cloud Pak for Data](#)” on page 874.

## What to do next

After the service is in use, you can download data and monitor performance. For more information, see “[Monitoring and downloading classifier data usage](#)” on page 856.

A natural language processing service is in one language. IBM supports a fixed set of languages. You can use multiple services simultaneously, either for different purposes or to support multiple languages for the same purpose.

If you use multiple services for taxonomy suggestions, each service requires a unique classifier configuration, classifier field, and classifier output fields. A classifier input field can be used in more than one classifier field. However, ensure that each classifier configuration updates different classifier target fields. Do not define multiple classifier configurations that update the same classifier target fields.

For object associations, you must configure a service for each object type and relationship that you want to support. For example, if you want to provide parent association suggestions to Control objects and child association suggestions to Risk objects, you need two services. You can have multiple services per object type. Each service requires a unique classifier configuration and classifier field. A classifier input field can be used in more than one classifier field.

## Configuring Watson Discovery

To use an IBM Watson Discovery service with OpenPages, you must configure it on IBM Cloud Pak for Data.

### About this task

Learn about cognitive technology, IBM Watson Discovery, and the Analyzer API. IBM provides extensive documentation, tutorials, and videos for IBM Watson Discovery. For more information, see the [IBM Watson Discovery documentation](#).

IBM Watson Discovery must be version 3.5 or greater.

For information about the format to use when you are building the training data, see [Data Format - OpenPages Classifier Models](#).

For information about training and integrating classifier models using a IBM Watson Discovery service with OpenPages, see [Training and integrating AI classifier models on OpenPages - Watson Discovery Analyze API](#).

## Configuring a Natural Language Understanding service on IBM Cloud

To use a Natural Language Understanding service with OpenPages, you must configure it on IBM Cloud (formerly called Bluemix).

## Before you begin

Learn about cognitive technology and IBM Cloud. IBM provides extensive documentation, tutorials, and videos for the Natural Language Understanding. For more information, see [Getting started with Natural Language Understanding](#).

## About this task

A Natural Language Understanding service is empty when you begin and must be trained for what you want to classify. If, for example, you want to help users correctly classify loss events to the correct Basel II categorization, you map short texts that they might write to the correct Basel II categories. The challenge when you create training data is to write short text inputs that reflect how users describe various loss events. The Natural Language Understanding service does not simply search through the texts, but instead interprets their meaning. When the meaning of a text is matched to a classification, it has a higher confidence score.

## Procedure

1. Create a IBM Cloud account if one does not already exist.
2. Log in, create the service, and get your service URL and API key. You need the service URL and API key later when you define a classifier configuration in OpenPages. Also make a note of the classifier instance ID.  
After you create an instance of the Natural Language Understanding service, you can view the service URL and API key by clicking **Manage** and **Show Credentials** from the left pane of the service dashboard.
3. Build the training data. For information about the format of the data, see [Data Format - OpenPages Classifier Models](#).
4. Train the model. For information about training, see [Training and integrating AI classifier models on OpenPages - Natural Language Understanding \(NLU\)](#).

## What to do next

Complete the remaining tasks that are described in [“Configuration overview for natural language classifier services” on page 852](#).

## Defining a classifier configuration

A classifier configuration defines connection information for an instance of IBM Watson Discovery or IBM Watson Natural Language Understanding.

## Before you begin

Configure the service that you want to connect to. For more information, see [“Configuring Watson Discovery” on page 853](#) and [“Configuring a Natural Language Understanding service on IBM Cloud” on page 853](#). Make a note of the API key and the ID of the natural language classifier instance that you created.

To do this task, you need the **Watson Mapping and Taxonomy Suggestions** application permission.

## Procedure

1. Click  > **Integrations** > **Mapping and Taxonomy Suggestions**.
2. Click **New Classifier**.
3. Complete the fields in the **Classifier Information** section.
  - a) Select **Watson Discovery Analyze API** or **Natural Language Understanding** in **Watson Service Type**.

- b) In **Type**, select Enumeration (taxonomy suggestions) or Association (object association suggestions).
  - c) In **Name**, enter a name.
  - d) In **Description**, enter descriptive information.
  - e) Enter a link in **Link**. The link is optional and for information purposes only. The default is <http://www.cloud.ibm.com>.
4. For a IBM Watson Discovery service, complete the fields in the **IBM Watson Discovery Service** section.
- a) Type your service URL in **URL for Request**. It is the URL to the IBM Watson Discovery Service on IBM Cloud Pak for Data that you configured.
  - b) Type the **Project ID**.
  - c) Type the **Collection ID**.
  - d) Enter a **Username**.
  - e) Enter a **Password**.
- If OpenPages and IBM Watson Discovery are both installed with the same IBM Cloud Pak for Data instance, you don't need to provide a password.
- f) Enter an **API Version**.
  - g) Click **Test Connection** to verify the connection settings.
5. For a Natural Language Understanding service, complete the fields in the **IBM Watson Natural Language Understanding Service** section. The person who trained the classifier model will have this information.
- a) Type your service URL in **URL for Request**. It is the URL to the Natural Language Understanding service on IBM Cloud.
  - b) In **API Key**, enter the API key of the Natural Language Understanding instance.
  - c) In **Model ID**, enter the identifier of the Natural Language Understanding classifier model.
  - d) Click **Test Connection** to verify the connection settings.
6. In the **Usage Information** section, in **Confidence Threshold** enter the lowest confidence score that a suggestion must meet.
7. If **Type** is set to Enumeration, in the **Field Settings** section you can choose up to three fields. The order of the fields is important. Select the top-level field first, then the second-level field, and so on.
8. If **Type** is set to Association, complete the **Association** section:
- a) In **Object Type**, select the object type that is associated, for example, SOXControl.
  - b) In **Association Type**, select Child or Parent.
  - c) In **Object Path**, enter a path to directories to search, for example, /Library.
  - d) In **Name Field**, specify the field that is displayed as the object's name after a user selects an object to associate, for example, System Fields.Name. Format is <Field Group>.<Field Name>.
  - e) In **Description Field**, specify the field that is displayed as the object's description after a user selects an object to associate, for example, System Fields.Description. Format is <Field Group>.<Field Name>.
9. Click **Create**.

## What to do next

Complete the remaining tasks that are described in [“Configuration overview for natural language classifier services” on page 852](#).

## Defining a classifier field

A classifier field contains the name of a classifier configuration and a classifier input field.

## Before you begin

Define a classifier configuration. For more information, see [“Defining a classifier configuration” on page 854.](#)

## About this task

A classifier field is a field whose **Data Type** is set to Classifier. Like other fields in OpenPages, you must add them to views and profiles. For more information, see [Chapter 10, “Fields and field groups,” on page 153.](#)

You can use FastMap to import and export classifier fields and the values for suggestions in associated classifier target fields. This is typically done during a migration process. Do not change the classifier field or the values for suggestions after you export and before you reimport.

## Procedure

1. Follow the instructions in [“Defining fields and adding them to field groups” on page 161.](#)
2. Click **New** to create a new field.
  - a) In **Data Type**, select Classifier.
  - b) In **Classifier Configuration Name**, enter the name of the classifier configuration that you created in [“Defining a classifier configuration” on page 854.](#)
  - c) In **Classifier Input Field**, enter the field that contains text to be interpreted by a service, for example, System Fields.Description. Format is <Field Group>. <Field Name>.
3. Save the field.

## What to do next

Complete the remaining tasks that are described in [“Configuration overview for natural language classifier services” on page 852.](#)

## Monitoring and downloading classifier data usage

After a natural language processing service has been implemented, you can monitor data usage and make improvements. You can view what users are searching for and what suggestions they select.

## Procedure

1. In IBM OpenPages with Watson, click  to open the Primary menu.
2. Click **Analytics**.
3. Click **Content**.
4. Click **Team content**, and then select **Platform Reporting**.
5. Click **Create > Create Report**.
6. On the **Create a report** page, select a template and click **Create**.
7. Under **Insertable objects**, click **Select a source**.
8. Click **General Reporting > Audit Trail > Classifier Audit Trail**.
9. Select one of the widget types depending on how you want to visualize the results of the query: **Test item**, **Block**, **Table**, **List**, **Crosstab**, or **Visualization**.
10. Drag the fields you want to see onto the widget page.

## What to do next

Use the results to improve the classifier. You can download the usage data as a CSV file and use it as a basis for new training data for the natural language processing service.

## Configuring a proxy URL for authentication (IBM Cloud)

If you connect to IBM Watson Natural Language Understanding through a proxy server, you might need to configure the authentication URL in OpenPages.

### About this task

By default, OpenPages authenticates with IBM Cloud by using `https://iam.cloud.ibm.com/identity/token`. If a different URL for IBM Cloud authentication is defined in your proxy server, you need to configure the URL in OpenPages.

For example, if your proxy server maps `https://iam.cloud.ibm.com/identity/token` to `https://www.myproxy.com/identity/token`, you need to configure OpenPages to use `https://www.myproxy.com/identity/token`.

### Procedure

1. Click  > **System Configuration** > **Settings**.
2. Click **Applications** > **Common** > **Configuration**. Change **Show Hidden Settings** to true.
3. Set **Applications** > **Common** > **Configuration** > **Allow Create and Delete Settings** to true.
4. Select the **Common** > **Security** folder, and then click **New Folder**.
5. In the **Name** field, type iam, and then click **Create**.
6. Select the iam folder, and then click **New Setting**.
7. Use the following values for the setting:
  - For the **Name**, type Authentication URL.
  - For the **Folder Path**, select **Common** > **Security** > **iam**.
  - For the **Value**, type the URL that this is defined on your proxy server, for example `https://www.myproxy.com/identity/token`.
8. Click **Create**.
9. Set **Applications** > **Common** > **Configuration** > **Allow Create and Delete Settings** to false.
10. Click **Applications** > **Common** > **Configuration**. Change **Show Hidden Settings** to false.

### Results

When OpenPages authenticates with IBM Cloud, it uses the URL that you specified in the **Common** > **Security** > **iam** > **Authentication URL** setting.

### What to do next

Verify the **URL for Request** field in the classifier configuration. For example, if you proxy maps the classifier URL to `https://www.myproxy.com/instances/<identifier>`, update the **URL for Request** field to use `https://www.myproxy.com/instances/<identifier>`.

## Custom Machine Learning Models

The Custom Machine Learning Models integration feature gives you the ability to deploy models and use input data from OpenPages fields to generate live insights and suggestions in OpenPages views. This feature also gives you the ability to customize how the insights are displayed in OpenPages.

To configure the model in OpenPages, you need the **Custom Machine Learning Models** application permission. If you don't have this permission, the  > **Integrations** > **Custom Machine Learning Models** menu item is not visible.

Models that are built that use Watson Studio AutoAI or developed by a data science team can be deployed to an AI service, and integrated into OpenPages.

You can choose from the list of available AI services when you configure your model in OpenPages. The list includes services such as IBM Watson Machine Learning on IBM Cloud, IBM Watson Machine Learning on Cloud Pak for Data, and IBM Natural Language Understanding on Cloud.

**Note:** Before you use an AI service, ensure that your company has selected a plan for that service that will support the volume of usage from within OpenPages.

The following models are examples of use cases that OpenPages supports:

- Models that display the insights that are found by running the model, such as Cognitive Controls and PII models.

Cognitive Controls models analyze text and return values for Who, What, When, Where, and Why.

PII models detect object text that contains Personally Identifiable Information (PII).

- Models that suggest values for fields. Fields can be set automatically or the user can set them manually.
- Models that suggest tags to categorize resources in OpenPages. Tags can be set automatically or the user can set them manually. Tagging allows users to find different resources that are related.

The following are prerequisites for configuring Custom Machine Learning Models in OpenPages:

- Models that are deployed on an AI service, such as IBM Watson Machine Learning, must be trained and tested by a data scientist. Testing ensures that the models have sufficient accuracies before they are deployed on the service.
- You must be familiar with the fields used as inputs to the model, the data types of the fields, and the order in which they are defined.
- You must be familiar with the model output format on the service.
- You must understand which components of the model's output you want to extract.
- You must understand JSONata (<https://try.jsonata.org>) syntax to extract relevant pieces of information.

When you are configuring a new model, you can save it at any time even if the configuration is incomplete, or you can cancel to exit without saving. When you have entered all of the required configuration data for a new configuration, and click **Create**, the configuration is validated. When the configuration successfully passes validation, it is marked as complete and can be used with views in OpenPages.

This video gives an overview of how to use the Custom Machine Learning Models integration feature:

[An overview of integrating custom AI models with OpenPages](#)

## What you need to configure your model

You need the credentials and other model details to configure your model in OpenPages.

Ask your data scientist to give you access to the model and to provide you with the following information:

- What service you are using for the model.
- Input field names, and the order in which the model requires them.
- Sample JSONata that represents the model output.

Other information that you need depends on the service you are using.

## Getting model information from IBM Watson Machine Learning

Get the credentials and other model details that you need to configure your model in OpenPages.

### Before you begin

Ask your data scientist to provide you with the information you need to access the IBM Watson Machine Learning model.

- Get the URL of the deployment.
- If you are using IBM Watson Machine Learning on IBM Cloud, get the API Key.

- If you are using IBM Watson Machine Learning on Cloud Pak for Data, get the username, and either the API key or password.

## Procedure

1. Enter the URL of your deployed model.
2. Click the **API Reference** tab and collect the following information:

- **Base Deployment URL**

Click the **API Reference** tab. The **Base Deployment URL** is at the beginning of the **Direct link Endpoint** URL up to /deployments.

- **Deployment ID**

Copy the **Deployment ID** from the side panel where it is displayed.

- **Space ID**

The **Space ID** is shown in the model's URL in your browser's address bar. Copy the part of the URL that follows &space\_id=.

## What to do next

You can now configure your model in OpenPages. For more information, see [“Setting up a connection to your model” on page 859](#).

## Getting model information from Natural Language Understanding

Get the credentials and other model details that you need to configure your model in OpenPages.

### Before you begin

Ask your data scientist to provide you with the model ID and the information you need to access the Natural Language Understanding model in IBM Cloud.

## Procedure

1. Log in to IBM Cloud.
2. Click  and select **Resource list**.
3. Click your service and select **Manage**.
4. In the **Credentials** section, expand the existing credentials that you are going to use or create your own.
5. Click the **Copy to clipboard** icon to copy the **API key** and the **URL** and paste them into a file on your computer.  
Save the file.

## What to do next

You can now configure your model in OpenPages. For more information, see [“Setting up a connection to your model” on page 859](#).

## Setting up a connection to your model

Set up a connection between OpenPages and your model instance, and configure your model in OpenPages.

### Before you begin

Get the credentials and other model details that you need to configure your model in OpenPages. For more information, see [“Getting model information from IBM Watson Machine Learning” on page 858](#) for

IBM Watson Machine Learning, or “[Getting model information from Natural Language Understanding](#)” on page 859 for Natural Language Understanding.

## Procedure

1. Log in to OpenPages.
2. Click  > **Integrations** > **Custom Machine Learning Models**.
3. Click **New model**.
4. Enter the following information:

### a. Name

Enter a unique identifier for the model.

### b. Label

Enter a label for the model that OpenPages users see in views.

Click **Translate** to translate the label.

If it is displayed, click  to populate translated values to languages. For more information, see “[IBM Watson Language Translator](#)” on page 847.

### c. Description

Enter the description of the model that you want users to see with the model insights.

This description is not displayed in views. It is displayed in the grid view that shows all the custom machine learning models.

Click **Translate** to translate the description.

If it is displayed, click  to populate translated values to languages. For more information, see “[IBM Watson Language Translator](#)” on page 847.

### d. Watson service type

Select the service type that you want to use.

### e. Insight type

Select how you want to use the model.

The page displays an image that shows an example of what the output looks like depending on the **Insight type** you select.

5. Enter the information in the **Access Parameters** section.

If you are using IBM Watson Machine Learning, see “[Setting access parameters for IBM Watson Machine Learning](#)” on page 860.

If you are using Natural Language Understanding, see “[Setting access parameters for Natural Language Understanding](#)” on page 861.

6. Click **Test Connection** to verify that OpenPages can connect to your model on IBM Cloud or IBM Cloud Pak for Data.

7. Click **Next** and continue with **Map inputs**.

For more information, see “[Configuring model inputs](#)” on page 862.

## Setting access parameters for IBM Watson Machine Learning

To connect to a model, you must set the access parameters. You set the access parameters as part of configuring a model on the **Access Parameters** section of the **Model access** page.

For more information about configuring models, see “[Setting up a connection to your model](#)” on page 859.

## About this task

The following instructions apply to IBM Watson Machine Learning on IBM Cloud and IBM Watson Machine Learning on Cloud Pak for Data.

## Procedure

1. If you are using IBM Watson Machine Learning on IBM Cloud, do the following steps:
  - a. **Authentication URL**  
Change this URL only if your organization is using a proxy. Only pass-through proxies are supported.
  - b. **API Key**  
Enter your IBM Cloud API key.
2. If you are using IBM Watson Machine Learning on Cloud Pak for Data, do the following steps:
  - a. **Authentication type**  
Select either **Username and API key** or **Username and password**.
  - b. **Username**  
Enter the user name to access the model.
  - c. If you chose **Username and API key**, select **API Key** and enter your Cloud Pak for Data API key.
  - d. If you chose **Username and password**, select **Password** and enter your password to access the model.
3. Enter the following information:
  - a. **Base Deployment URL**  
Enter the deployment URL of your model.
  - b. **Deployment ID**  
Enter the deployment ID of your model.
  - c. **Space ID**  
Enter the space ID of your model.
  - d. **API Version**  
Enter the API version of the **Watson service type**. To get the version, go to <https://cloud.ibm.com/apidocs/machine-learning-cp#versioning>.

## Setting access parameters for Natural Language Understanding

To connect to a model, you must set the access parameters. You set the access parameters as part of configuring a model on the **Access Parameters** section of the **Model access** page.

For more information about configuring models, see “[Setting up a connection to your model](#)” on page [859](#).

## Procedure

Enter the following information in the **Access Parameters** section:

- a. **Authentication URL**  
Change this URL only if your organization is using a proxy. Only pass-through proxies are supported.
- b. **API Key**  
Copy the API key that you obtained from the model information in IBM Cloud and paste it into **API Key**.
- c. **Base Deployment URL**

Copy the URL that you obtained from the model information in IBM Cloud and paste it into **Base Deployment URL**.

d. **API Version**

Enter the API version of the **Watson service type**. To get the version, go to <https://cloud.ibm.com/apidocs/natural-language-understanding#versioning>.

- e. If you selected **Natural Language Understanding on Cloud** as the **Watson service type**, enter a **Configuration string** that specifies the **Natural Language Understanding on Cloud** text analytics feature to be used.

## Configuring model inputs

After you set up a connection to your model, configure the inputs for the model. The inputs are the fields in OpenPages that contain the data that you want the model to process.

### About this task

Ask your data scientist to provide you with the inputs that are needed for the model you are using.

You can use one OpenPages object type per model or you can select all object types to use multiple object types with the model.

### Procedure

1. In the **Object type** section of the **Map inputs** page, do one of the following steps:

- Select the object type that you want to use with the model.
- Select **Select all object types** if you want to use the model with multiple object types.

When **Select all object types** is selected, only System fields are available for selection.

2. Do one of the following steps:

- Select **Manual** so that the user can control when the model runs.
- Select **Automatic** to run the model when all of the required fields are set.

3. Map the inputs that your model needs to the OpenPages fields that contain the data.

Ensure that your input fields meet the following requirements:

- At least one required field is specified.
- The type of each OpenPages field must match the type of the model input field it is mapped to.
- Fields must be listed in the order that the model expects, if applicable. If you need to rearrange the list, you can drag the fields to change the order.

Create a row for each input that your model needs. Click **Add input** to add a row.

- **Model input fields**

Enter the name of a model input field.

If your model does not specify input field names, you can specify your own field names.

- **OpenPages fields**

Select the field that contains the input data that you want to send to the model. For example, you might map **Description** to **Description(System Fields:Description)**.

4. Click **Next** and continue with **Map outputs**.

For more information, see “[Configuring model outputs](#)” on page 863.

# Configuring model outputs

After you map the inputs, you need to configure the outputs that OpenPages receives from the model.

## About this task

Define how to parse the model outputs to collect the insights that you want to display in OpenPages. The model outputs use JSON format. To parse the JSON, OpenPages uses a library that is named JSONata. For more information about parsing the model outputs, see [“Parsing model outputs with JSONata” on page 864](#).

For more information about how OpenPages processes model outputs when you set the **Insight type** on the **Model access** page to **Set fields** or **Set tags**, see [“How OpenPages processes model outputs” on page 870](#).

## Procedure

1. In the **What type of output is the model extracting** section of the **Map outputs** page, do one of the following steps:
  - Select **Single insight** to have a single value returned per output field.
  - Select **Multiple insights** to have a list of values returned per output field.

The list must have the same number of values for each output field.
2. Define each output in the order that you want them displayed in OpenPages. Click **Add output** to add a row.

- **Output label**

Enter a name for the output.

- **JSONata string**

Enter the JSONata string to extract the required information that is sent from the model to OpenPages in JSON format.

In step 1, if you select **Multiple insights**, the model must return a list of outputs. Some JSONata expressions return lists when multiple values are found, but just a single node value when only one entry is found. Ensure that you test your expressions in a scenario where a single value is returned in the JSON. If necessary, modify the expression to ensure a list, rather than a single node value, is returned for this scenario.

For more information about creating JSONata expressions, see [“Parsing model outputs with JSONata” on page 864](#).

- **Target field**

If you set **Insight type** on the **Model access** page to **Set fields**, at least one output must have a target field specified. For outputs with a target field, enter the name of the field that the suggested value is applied to.

- **Tag source**

If you set **Insight type** on the **Model access** page to **Set tags**, you must select **Source** in the **Target source** column for one of the outputs to identify it as the source of the tag suggestions.

If you need to rearrange the list, you can drag the fields to change the order.

3. Optional: In the **Confidence score settings** section, do one of the following steps:

- If a single insight is selected, define the JSONata expression that returns a single confidence score.
- If a list of insights is selected, define the JSONata expression that returns a list of confidence scores.

The JSONata expression is applied to the model output to extract the confidence score for the insight. The expression must return a value from 0 to 100.

When you enter a value for **Confidence score settings**, the **Set minimum confidence threshold for display** section is displayed.

4. In the **Set minimum confidence threshold for display** section, enter a number from **0** to **100** to specify the minimum percentage at which to display insights to the user.

If you don't specify a value, all insights are displayed to the user up to a maximum of 20 insights in the order in which the model returns them.

5. If you set **Insight type** on the **Model access** page to **Set fields** or **Set tags**, do one of the following steps:

- If you want the user to be able to choose which suggestions to apply to the fields or tags, select **User set**.
- If you want the suggestions to be automatically applied when the confidence threshold is met or exceeded, select **Automatically set**.

If you select **Automatically set**, the **Minimum confidence threshold for setting tags and fields** section is displayed. Enter the lowest confidence score at which you want OpenPages to automatically set fields or tags. You can enter a value of **0** to **100**.

If you don't specify a minimum confidence threshold, the first entry in the list of returned values is used to set the field.

6. Optional: If you set **Insight type** on the **Model access** page to **Set tags** and you want OpenPages to create any new tags suggested by the model, select **If the user chooses to apply a suggested tag, create the tag if it doesn't exist**.

If **User set** is selected, the user can choose the tags they want to create and apply.

If **Automatically set** is selected, any new tags suggested by the model that meet or exceed the **Minimum confidence threshold for setting tags and fields** value are created and applied.

If you don't select **If the user chooses to apply a suggested tag, create the tag if it doesn't exist**, suggestions for tags that don't exist in OpenPages are filtered out from the model results before they are displayed to the user.

7. Optional: If you set **Insight type** on the **Model access** page to **Set fields**, select **Overwrite existing values in the fields** if the following conditions are true:

- You set **Insight type** on the **Model access** to **Set fields**.
- You want fields that already have values to be overwritten with the output from the model.

8. Click **Next** and continue with **Guidance**.

For more information, see “[Configuring user guidance](#)” on page 871.

## What to do next

You can now add the model to a view. For more information, see “[Adding a model to a view](#)” on page 872.

## Parsing model outputs with JSONata

OpenPages uses the JSONata expression language to parse the JSON from the model outputs.

Different models can have different output structures. JSONata queries and transforms the output of the model so that the output can be used by OpenPages, regardless of the model structure.

OpenPages uses the open source Java version of JSONata, JSONata4Java that does not implement all of the JSONata functions. For more information, see [the readme in the IBM JSONata4Java Github repository](#).

## About this task

The procedure uses an example to demonstrate how to parse model outputs.

The model that is used in the example generates the following output:

```
{
 "predictions": [
 {
 "results": {
 "Controls": [
 {
 "text": "No recommendations available",
 "score": 0,
 "name": "Not Found"
 }
],
 "Class": [
 {
 "score": 0.8766618371009827,
 "label": "Technical"
 }
],
 "Priority": [
 {
 "score": 0.9162724614143372,
 "label": "P1"
 }
],
 "LDA": [
 {
 "score": 0.4810614287853241,
 "label": "Authorization"
 },
 {
 "score": 0.31226786971092224,
 "label": "Configuration"
 },
 {
 "score": 0.13503773510456085,
 "label": "System"
 },
 {
 "score": 0.017938677221536636,
 "label": "Policy"
 },
 {
 "score": 0.017931180074810982,
 "label": "Information"
 },
 {
 "score": 0.017895007506012917,
 "label": "Control"
 },
 {
 "score": 0.01786813512444496,
 "label": "Security"
 }
],
 "Quali": [
 {
 "semantic_roles": [
 {
 "sentence": "Product Management will verify test cases via Post
Launch Monitoring.",
 "subject": {
 "text": [
 "Product Management"
]
 },
 "action": {
 "text": [
 "will verify"
]
 },
 "object": {
 "text": [
 "Post Launch Monitoring",
 "test cases"
]
 },
 "when": {
 "text": false
 }
 }
]
 }
]
 }
]
]
}
```

```

 {
 "sentence": "Product PQ testing and analysis is also determined and performed on a quarterly basis.",
 "subject": {
 "text": [
 "Product PQ testing and analysis"
]
 },
 "action": {
 "text": false
 },
 "object": {
 "text": [
 "a quarterly basis"
]
 },
 "when": {
 "text": [
 "quarterly"
]
 }
 }
],
 "rating": "No Review Needed",
 "feedback": null,
 "rules": {
 "Abbreviation": true,
 "Title and Description Relevance": false,
 "Jargon": false,
 "Spelling Errors - Minor": false,
 "Spelling Errors - Moderate": false,
 "URLs": false,
 "Word Count - Low # of Words": false,
 "Word Count - Too many Words": false,
 "Word Count - Medium # of Words": false,
 "Insufficient information explaining who, what, why, how": false,
 "Conditional Words": false
 },
 "errors": [],
 "cond": []
}
],
"semantic_roles": [
{
 "sentence": "Product Management will verify test cases via Post Launch Monitoring.",
 "subject": {
 "text": [
 "Product Management"
]
 },
 "action": {
 "text": [
 "will verify"
]
 },
 "object": {
 "text": [
 "Post Launch Monitoring",
 "test cases"
]
 },
 "when": {
 "text": false
 }
},
{
 "sentence": "Product PQ testing and analysis is also determined and performed on a quarterly basis.",
 "subject": {
 "text": [
 "Product PQ testing and analysis"
]
 },
 "action": {
 "text": false
 },
 "object": {
 "text": [
 "a quarterly basis"
]
 },
}
]

```

```
 "when": {
 "text": [
 "quarterly"
]
 }
 },
 "questions": [
 {
 "sentence": "Product Management will verify test cases via Post Launch Monitoring. Product PQ testing and analysis is also determined and performed on a quarterly basis.",
 "full_question": "Who performs the control?",
 "question": "Who",
 "text": "product management"
 },
 {
 "sentence": "Product Management will verify test cases via Post Launch Monitoring. Product PQ testing and analysis is also determined and performed on a quarterly basis.",
 "full_question": "What is performed?",
 "question": "What",
 "text": "product pq testing and analysis"
 },
 {
 "sentence": "Product Management will verify test cases via Post Launch Monitoring. Product PQ testing and analysis is also determined and performed on a quarterly basis.",
 "full_question": "When or how frequently is the control performed?",
 "question": "When",
 "text": "quarterly"
 },
 {
 "sentence": "Product Management will verify test cases via Post Launch Monitoring. Product PQ testing and analysis is also determined and performed on a quarterly basis.",
 "full_question": "Where is the control performed?",
 "question": "Where",
 "text": "product pq testing and analysis is also determined and performed on a quarterly"
 },
 {
 "sentence": "Product Management will verify test cases via Post Launch Monitoring. Product PQ testing and analysis is also determined and performed on a quarterly basis.",
 "full_question": "Why is this performed?",
 "question": "Why",
 "text": "product pq testing and analysis is also determined and performed on a quarterly basis ."
 }
],
 "cutoff": 0.06,
 "scores": [
 {
 "score": 0.47622546553611755
 },
 {
 "score": 0.4898279309272766
 },
 {
 "score": 0.3327782452106476
 },
 {
 "score": 0.25064486265182495
 },
 {
 "score": 0.3405856490135193
 }
]
}
```

In the example, the following information is displayed in the output:

- The model components are Who, What, When, Where, and Why.
  - The model insights for each component are displayed as the text associated with each component.
  - The confidence scores for each component are displayed.

## Procedure

1. Get the JSON model output from your data scientist.
2. Copy the JSON and paste it into <https://try.jsonata.org>.
3. Find the JSONata string that can extract the information that you need.

For the example, you can use the string `predictions.results.questions.question`. You can see that the output of this string is a list of ["Who", "What", "When", "Where", "Why"].

The screenshot shows the try.jsonata.org interface. On the left, there is a large JSON code block representing the model output. On the right, there are two panels: one for the JSONata query and one for the resulting output. The JSONata query panel contains the string `predictions.results.questions.question`. The resulting output panel shows the extracted list: `[ "Who", "What", "When", "Where", "Why" ]`.

```
predictions.results.questions.question
```

```
["Who", "What", "When", "Where", "Why"]
```

Figure 87. Extracting a list of questions

For the confidence score, you can use the string `predictions.results.scores.score` to extract a list of the scores.

The screenshot shows the try.jsonata.org interface. On the left, there is a large JSON code block representing the model output. On the right, there are two panels: one for the JSONata query and one for the resulting output. The JSONata query panel contains the string `predictions.results.scores.score`. The resulting output panel shows the extracted list of scores: `[ 0.4762254655361, 0.4898279309273, 0.3327782452106, 0.2506448626518, 0.3405856490135 ]`.

```
predictions.results.scores.score
```

```
[0.4762254655361, 0.4898279309273, 0.3327782452106, 0.2506448626518, 0.3405856490135]
```

Figure 88. Extracting a list of scores

4. Get the model text that is associated with each of the components and scores by using the string `predictions.results.questions.text`.

The screenshot shows a JSONata editor interface. At the top, the path 'predictions.results.questions.text' is entered. To the right, the version '2.0.2' is displayed. The main area shows a JSON array with one item, containing several strings related to product management and testing.

```
[{"product management", "product pq testing and analysis", "quarterly", "product pq testing and analysis is also determined and performed on a quarterly", "product pq testing and analysis is also determined and performed on a quarterly basis ."}]
```

Figure 89. Getting the model text for components and scores

## What to do next

You define the outputs in the order in which you want them displayed in OpenPages. When you configure the outputs, you specify the JSONata string that extracts the specific components from the model. You also specify a JSONata string for the Confidence score.

### Edit model

Edit the machine learning model to take advantage of real-time predictions.

The screenshot shows the 'Map outputs' configuration page. On the left, a sidebar lists options: Model access (selected), Inputs, Outputs (selected), and Guidance. The main area is titled 'Map outputs' and contains the following fields:

- What type of output is the model extracting? \***: Single insights (radio button)
- Output label \***: Question
- JSONata string \***: predictions.results.questions.question
- Answer**: predictions.results.questions.text
- Add output**: A button with a plus sign.
- Confidence score settings**: JSONata string: predictions.results.questions.score.score.(#\$\*100)

At the bottom, there are 'Cancel', 'Previous', and 'Next' buttons. The 'Next' button is highlighted in blue.

Figure 90. An example of a **Map outputs** page

For more information about defining model outputs, see “[Configuring model outputs](#)” on page 863.

After the model is added to the **Description** field in the **Task View for Controls**, the example configuration that is shown in the preceding figure generates the following result in OpenPages.

The screenshot shows the IBM OpenPages with Watson interface. At the top, there's a navigation bar with icons for home, search, and user profile. Below the navigation is a breadcrumb trail: Home > RB-01-Risk0... > MyControlTaskView. The main content area is titled 'Control' and shows a card for 'RB-01-Risk00189\_CON\_...' with status indicators: Design Effectiveness (Not Determined), Operating Effectiveness (Not Determined), and Status (Awaiting Assessment). Below this, there are tabs for Task, Activity, and Admin, with Task selected. A search bar and a 'Reveal editable fields' button are also present. The main form contains sections for General (Name: RB-01-Risk00189\_CON\_00000001, Description: Product management will verify test cases via post-launch monitoring, Status: Awaiting Assessment), Control Activities (Control Owner: John Adams, Control Attester, Classification: Not Determined), Control Method, Control Type, Domain, Frequency, and Control Assessment (Design Effectiveness: Not Determined, Operating Effectiveness: Not Determined). To the right of the main form is a sidebar titled 'Cognitive Controls Model insights'. It includes a section for 'When' (post - launch monitoring, Confidence: 80.68%), 'Where' (post - launch monitoring, Confidence: 49.04%), 'Who' (product management, Confidence: 44.25%), 'What' (post - launch monitoring, Confidence: 33.32%), and 'Why' (product management will verify test cases via post - launch monitoring, Confidence: 32.90%).

Figure 91. An example of a Control view that displays the **Insights** panel

## How OpenPages processes model outputs

If you choose **Set fields** or **Set tags** as the **Insight type** on the **Model access** page, OpenPages might filter or convert the suggestions that are returned from the model.

### Set fields

If you set **Insight type** on the **Model access** page to **Set fields**, the following suggestions are filtered out:

- Suggestions that have a data type that is not compatible with a target field.
- Suggestions that have target enumeration values that don't exist in the enumeration type.

### Set tags

If you set **Insight type** on the **Model access** page to **Set tags**, tags are suggested when the following conditions are met:

- The tag that the model returns matches an existing OpenPages tag. For more information, see ["How OpenPages tags and tags from the model are compared" on page 870](#).
- The OpenPages tag is not yet associated with the resource.
- The OpenPages tag is enabled.

Also, new tags are suggested if the configuration allows tags to be created in OpenPages.

## How OpenPages tags and tags from the model are compared

The model might not return tag suggestions in the same way that they are defined in OpenPages. For example, the model might return the tag `Requires Attention` as `RequiresAttention`. To ensure that the suggestions that the model returns match the appropriate tags in OpenPages, the comparison process includes the following steps:

- The comparison of model suggestions to OpenPages tags is case-insensitive.

- Underscores are removed from model suggestions.
- Spaces are removed from OpenPages tags. Other characters that are sometimes used as separators, such as underscores, are not removed.

If a tag returned by the model does not exist in OpenPages and **When the user choose to apply a suggested tag, create the tag if it doesn't exist** is selected, the tag is created and applied in OpenPages. Otherwise, suggestions for tags that don't exist are filtered out from the model results.

When a tag is created, the following formatting is applied:

- The letter at the beginning of each word is capitalized.
- Underscore characters are replaced by spaces.

## Configuring user guidance

After you map the outputs, you need to configure the guidance that OpenPages provides to the user when the model returns the outputs.

### About this task

Define the notification messages and model description to provide to the user, and how to display the insights to the user.

The page displays an image that shows an example of what the output looks like depending on your specifications.

### Procedure

- In the **Notifications** section of the **Guidance** page, define each notification message that you want displayed to the user. Click **Add rule** to add a notification message.

- Model criteria**

Select **1 or more model outputs**, **No model output**, or **Custom model output**.

If you select **Custom model output**, specify each condition under which the notification is displayed.

- Output**

Select the output field that you want to base the condition on. The output field definition must always return a single numeric value.

- Operator**

Select the operator to use when the model is comparing the value of the output field against the set value. You can select **Equal**, **Greater than or equal**, or **Less than or equal**.

- Value**

Enter the numeric value to compare against the output field value.

- Icon**

Select the icon that is displayed with the notification text. You can choose **Success**, **Info**, or **Warning**, or you can select **No icon** if you don't want an icon to be displayed.

- Notification text**

Enter the text that you want to appear when the output meets the model criteria.

Click **Translate** to translate the notification text.

If it is displayed, click  to populate translated values to languages. For more information, see “IBM Watson Language Translator” on page 847.

If you drag the rows to change the order of the notification messages, the notifications and how they are displayed to the user do not change. However, the rules are evaluated from first to last, and the first rule that applies is used without further evaluation.

2. In the **Style** section, select a text style for each of the output fields.

Select **Header**, **Body**, **Label**, or **Hidden**.

If you select the **Label** style for a numeric field, the **Label** text you specified is displayed and the number is displayed as a confidence score.

If you select the **Hidden** style, the field is not displayed in the UI. However, you can use the field to create a calculation, by using JSONData, to use with custom alerts.

3. Click **Create**.

## What to do next

You can now add the model to a view. For more information, see [“Adding a model to a view” on page 872](#).

## Adding a model to a view

After you configure a model, add the model configuration to a view. Depending on your model configuration, a model either runs automatically or a user can choose to run the model from the view. The results are displayed to the user in a side panel of the view.

### Before you begin

Ensure that you have a custom view to add the model to and that it is the default view. For more information about creating a custom view, see [“Creating custom views” on page 255](#).

### Procedure

1. Click  > **Solution Configuration** > **Views**.
2. Select a custom view for the object type that you specified when you configured the model. For example, if the model is configured for Controls, you can select a Controls task view.
3. Select an input field to associate with the model. The field must be identified as an input field in the model configuration.

For example, if you selected **Description(System Fields:Description)** as an input field in the model configuration, select the **Description** field.

When an input field is associated with a model, the  icon is displayed with the field when a user opens the view. Users can perform one of the following tasks:

- If the model is configured to run automatically, the model runs after the user modifies the input field. To view the output from the model, the user clicks the  icon with the input field.
- If the model is configured to run manually, the model runs when the user clicks  associated with the input field.

At least one input field must be associated with the model.

4. Click **Model configuration** and select the model.

5. Click **Done**.

The  icon is displayed with the field when a user opens the view.

6. Repeat steps 3 to 5 for each additional input field that you want to associate with the model.

7. Click **Publish**.

# Testing a model

After you add a model to a view, you can test the model.

## About this task

Use the following instructions to test a model.

## Procedure

1. Open a view for an object that includes the model configuration. For example, if you added the model to a Creation View, create a new object of that type.

Ensure that the view you added the model to is displayed as the **View name**. If it isn't, ensure that the stage on the workflow doesn't have a task override specified.

2. Do one of the following steps:

- If you configured the model to run automatically, enter or modify values for the input fields that the model requires. The insights icon  identifies an input field. If you configured notifications, a notification is displayed when the model finishes running.

If your configuration is using the **Set fields** or **Set tags** insight type, and you selected **Threshold set**, one of the following actions occurs:

- If you specified a minimum confidence threshold, **Set minimum confidence threshold for setting tags and fields**, the fields or tags are automatically set if the threshold you specified is met or exceeded.
- If you did not specify a minimum confidence threshold and the model is configured to set fields, the first entry in the list is automatically applied to the field.
- If you did not specify a minimum confidence threshold and the model is configured to set tags, all tags are applied to the object.

If you want to see the results, click the  associated with the input field you modified. The results are displayed in a side panel.

- If you configured the model to run manually, click the  associated with an input field to run the model. If you configured notifications, a notification is displayed when the model finishes running. The results are displayed in a side panel.

If your configuration is using the **Set fields** or **Set tags** insight type, and you selected **Threshold set**, one of the following actions occurs:

- If you specified a minimum confidence threshold, **Set minimum confidence threshold for setting tags and fields**, the fields or tags are automatically set if the threshold you specified is met or exceeded.
- If you did not specify a minimum confidence threshold and the model is configured to set fields, the first entry in the list is automatically applied to the field.
- If you did not specify a minimum confidence threshold and the model is configured to set tags, all tags are applied to the object.

In the following figure, a model uses the **Description** field for input. When you click , the insights that the model generated from the **Description** are displayed in the **Insights** panel.

The screenshot shows the 'Loss Event' view for the entry 'Abrucca Limited LE\_0001'. Key details include:

- Name:** Abrucca Limited LE\_0001
- Description:** This loss is due to mismanagement of funds
- Owner:** John Adams
- Loss Event Categorization:**
  - Causal Category: [empty]
  - Risk Category: [empty]
  - Business Line: [empty]
  - Causal Subcategory: [empty]
  - Risk Sub-Category: [empty]
  - Risk Example: [empty]
- Loss Event Dates:**
  - Discovery Date: 3/26/2023
  - Recognition Date: [empty]

**Suggestions**

Risk Category	Risk Sub-Category	Risk Example	Confidence
Clients, Products and Business Practices	Improper Business or Market Practices	Improper trade / market practices	23.83%
Internal Fraud	Theft and Fraud	Misappropriation of assets	14.60%
Clients, Products and Business			

Figure 92. Example of using a view to test a **Set fields** model

## Importing a certificate for Watson services on IBM Cloud Pak for Data

If you're integrating with Watson services on IBM Cloud Pak for Data and you're using a self-signed certificate or an unknown CA certificate, you must import a certificate from IBM Cloud Pak for Data to the local truststore. The certificate is needed to build a secure connection between the OpenPages with Watson application servers and the services that are running on IBM Cloud Pak for Data.

### About this task

This task applies to OpenPages with Watson.

This task applies only when you're using a self-signed certificate or an unknown CA certificate in IBM Cloud Pak for Data.

### Procedure

- Get the certificate from IBM Cloud Pak for Data and copy it to the OpenPages with Watson application server.
- Log on to the OpenPages with Watson application server.
- Import the certificate to WebSphere Liberty by running the following command:

```
keytool -importcert -v -alias <CERTIFICATE_ALIAS> -file <CERTIFICATE_NAME> -keystore <STORE_PATH> -storetype PKCS12 -storepass <STORE_PASSWORD>
```

Where:

- <CERTIFICATE\_ALIAS> is the alias of the certificate that you received from IBM Cloud Pak for Data.
- <CERTIFICATE\_NAME> is the file name of the certificate.
- <STORE\_PATH> is the full path and file name of the truststore on the application server. For example: <OP\_HOME>/wlp-user/servers/<server\_name>Server<#>/resources/security/key.p12

- <STORE\_PASSWORD> is the password of the truststore on the application server.

For more information, see [Adding trusted certificates in Liberty](#) in the WebSphere Liberty documentation.

4. Restart the OpenPages with Watson services.
5. Repeat these steps on each application server.



# Chapter 34. IBM OpenPages Data Privacy Management

IBM OpenPages Data Privacy Management (DPM) solution is used by an organization to aid in complying with data privacy regulations. With DPM, you can maintain an inventory of all private data across the organization within OpenPages by using an integration with Watson Knowledge Catalog.

This video provides an overview of IBM OpenPages Data Privacy Management.

## [IBM OpenPages Data Privacy Management Overview](#)

The integration imports metadata from Watson Knowledge Catalog into OpenPages. The data itself is not imported.

**Note:** To integrate with Watson Knowledge Catalog, you must meet the following prerequisites:

- You must have a Watson Knowledge Catalog instance on IBM Cloud Pak for Data.
- You must have a fresh installation of OpenPages 8.3 or later.

Before you import data from Watson Knowledge Catalog, do the following tasks:

- In Watson Knowledge Catalog, create at least one catalog. Add assets to the catalog.
- In Watson Knowledge Catalog, classify the assets. Make a list of the classifications that you want to import into OpenPages.
- Optional: In OpenPages, create a questionnaire template to use for privacy assessments.

When you import data from Watson Knowledge Catalog, the data is mapped to the following object types in OpenPages:

<i>Table 251. Watson Knowledge Catalog content mapping</i>	
<b>Watson Knowledge Catalog content...</b>	<b>Is loaded as a...</b>
Project	System
Asset	Asset

When OpenPages imports data from Watson Knowledge Catalog, it does the following tasks:

- For projects, the import process does the following tasks:
  - Identifies projects that contain assets with one or more of the classifications that you configured for the import.
  - If the project does not exist in OpenPages, the import process creates a new System object.
- For assets, the import process does the following tasks:
  - Identifies assets with one or more of the classifications that you configured for the import.
  - If the asset does not exist in OpenPages, the import process creates a new Asset object and starts the Privacy Impact Assessment workflow.
    - If the asset is part of a project, the Asset object is added as a child of the System object.
    - If the asset exists in OpenPages, the import process checks for updates, such as links to other projects and changes to the status of the asset.

When projects or assets change, the import process makes the following updates:

- If a project is deleted from Watson Knowledge Catalog or if it no longer contains classified assets, the System object remains in OpenPages. The import process changes the Status field on the System object to **No Longer Private**.
  - If an asset no longer matches the classifications that you configured for the import, the import process changes the Status field on the Asset object to **No Longer Private**.
- If an asset is deleted from Watson Knowledge Catalog, the import process changes the Status field on the Asset object to **Deleted**.

**Note:** The import process does not update names. If an asset is renamed in Watson Knowledge Catalog and you want to use the new name in OpenPages, manually delete the Asset object and then re-import it into OpenPages.

## Configuring the Watson Knowledge Catalog connector

---

Configure the import of Watson Knowledge Catalog metadata into IBM OpenPages with Watson.

### Before you begin

- Get the following information:
  - Your Watson Knowledge Catalog credentials. You can use an API key and username or a password and username. The username must have access to the data that you want to import. If you want to use an API key, see [Generating an API key](#).
  - Your IBM Cloud Pak for Data URL.
  - The classifications in Watson Knowledge Catalog that you want to import.
- If you're using IBM OpenPages for IBM Cloud Pak for Data, see [Importing a certificate into the local truststore on IBM OpenPages for IBM Cloud Pak for Data..](#)
- If you're using OpenPages with Watson and you're using a self-signed certificate or a certificate authority (CA) that is not known, you must import an SSL certificate from Watson Knowledge Catalog. For more information, see “[Importing a certificate for Watson services on IBM Cloud Pak for Data](#)” on page 874.

### About this task

To do this task, you need the following application permissions:

- **SOX > Administration > Scheduler**

### Procedure

1. Log in to OpenPages.
2. Click  **Solution Configuration > Scheduler**.
3. Click the **Data Privacy WKC Import** job.
4. Click **Edit**.
5. Configure the connector:

- Enter your credentials.

If you want to use an API key, enter your Watson Knowledge Catalog API key and username, and then type undefined in the **Password** field.

If you want to use a password, enter your Watson Knowledge Catalog username and password, and then type undefined in the **API Key** field.

- Click **Base URL** and type your IBM Cloud Pak for Data URL.
- Verify the value in the **Parent Entity Path** field. The objects that are created during the import are created under this path. You can use the default or specify another path.

- Click **WKC Classifications** and type a comma-separated list of classifications. Assets with these classifications will be imported. The classification names must match the names in Watson Knowledge Catalog.

For example, Sensitive Personal Information, Personally Identifiable Information, Electronic Protected Health Information

- If you want to reload all data, click **Reload All** and set it to true. if you want to import only new data, set it to false.
- In the **Schedule** section, click **Edit**. Set the schedule for the import.

#### 6. Click **Done**.

The connector is configured and the import is scheduled.

#### 7. If you want to import data from Watson Knowledge Catalog now, click the checkbox next to the **Data Privacy WKC Import** job and then click **Start Job** ▶.

### What to do next

To see the progress of an import, go to  > **Solution Configuration** > **Scheduler**. click the **Data Privacy WKC Import** job, and then click the **Executions** tab. Click a process to view the log.



---

# Chapter 35. IBM OpenPages IT Governance with RiskLens

IBM OpenPages IT Governance includes an integration with the cyber risk quantification analysis platform RiskLens.

Within the RiskLens platform, users record the assets and threats to include in scenarios, and then populate these objects in accordance with the FAIR (Factor Analysis of Information Risk) method by using data helpers that are provided in RiskLens for guidance.

In OpenPages, users specify the risks to send to RiskLens for inclusion within a risk assessment in RiskLens. An OpenPages object can be associated to one or more scenarios within RiskLens.

In RiskLens, Monte Carlo simulations are performed on the risks and results are generated.

When the scheduled job in OpenPages runs, the loss exposure metrics that were generated by the Monte Carlo simulations are pulled into OpenPages for use throughout the application.

The scheduled job in OpenPages also pulls updated data from RiskLens when risk assessments are modified in RiskLens.

## Prerequisites

To use the connector, you must meet the following prerequisites:

- You must have a RiskLens subscription. Work with RiskLens to set up access. For more information, contact RiskLens.
- You must install the RiskLens connector. For more information, contact IBM OpenPages Support.

## Setting up the integration with RiskLens

To set up the integration, you need to do the following tasks:

- In RiskLens, create Assets, Threats, and Scenarios by using data helpers.
- Configure the integration. See [“Configuring the RiskLens connector” on page 882](#).

When the RiskLens job runs, it does the following tasks:

- Identifies risk objects in OpenPages that have the **Perform Risk Analysis** field set to Yes and sends them to RiskLens.
- If a risk assessment does not exist in RiskLens for the risk, the job creates one.
  - The Assessment Name in RiskLens is populated with the Risk Name and the Resource ID of the Risk.
  - The Assessment Purpose field in RiskLens is populated with the Description field from the Risk object.
  - The Risk Status field on the risk object is set to "Awaiting Analysis."
- For risk assessments that are associated with scenarios in RiskLens where a Monte Carlo simulation has been run and the status of the risk assessment is **Current**, the RiskLens job does the following steps:
  - Retrieves the loss exposure metrics that were generated from the simulation and stores them in fields within the OPSS-RiskLens field group.
  - The Request State is changed to "Assessment Received."
  - The Analysis Last Run field is updated with the last date that the risk object was updated.
  - The Scenarios field is populated with the names of the scenarios that were analyzed within RiskLens.
- If risk assessment results are not yet available for a risk, the Request Status field on the risk object is "Awaiting Analysis."

## Notes

If you change the Description field of a risk in OpenPages, the Assessment Purpose field in RiskLens is not updated. But you can update the field by using the RiskLens web client.

Similarly, if you edit the Assessment Purpose field in RiskLens, the Description field in OpenPages is not updated automatically. But you can edit the Description in OpenPages.

If you delete either the risk object in OpenPages or the Risk Assessment in RiskLens, note the following points:

- The job continues to run successfully. But the link between the risk and the risk assessment no longer exists. No data will be pushed or pulled for the risk or risk assessment.
- No notifications are sent when a risk or risk assessment is dropped.

## Using a different object type with RiskLens

By default, the integration is set up for the Risk object type. But you can use other object types.

- Add the OPSS-RiskLens field group to the object.
- Add that object to the **Object Types** field in the job configuration.
- Reset the priority of the RiskLens views so that they take priority for the object type. Or, create new views that include the OPSS-RiskLens field group.

## Configuring the RiskLens connector

---

Configure the import of RiskLens data into IBM OpenPages with Watson.

### Before you begin

To connect to RiskLens, you need all of the following items:

- Your RiskLens client ID and secret.

### About this task

To do this task, you need the following application permissions:

- **SOX > Administration > RiskLens Feed**
- **SOX > Administration > Scheduler**

### Procedure

1. Log in to OpenPages as an administrator.
2. Reset the priority for the RiskLens views so that they take priority for the Risk object type for the ITG RiskLens Master profile:
  - a) Click  > **Solution Configuration > Views**.
  - b) In the search box, type `risklens`.
  - c) For each view, click  and change the priority to 1 for the **ITG RiskLens Master** profile.

The screenshot shows the IBM OpenPages interface with the title bar "IBM OpenPages with Watson". In the top navigation bar, there are icons for Home, Views, and other settings. The main area displays a table titled "Views (4)" with a search bar and filters. The table columns are Name, Description (optional), Object Type, View Type, Priority, and Published. Four rows are listed, all of which are Risk (SOXRisk) objects and Task View Types. The first three rows have a Priority of 6, while the fourth row has a Priority of 2. To the right of the table, a modal window titled "Edit view" is open. It has tabs for "Overview" (selected) and "Rules". Under "Matching information", there is a section for "View Priority" with a dropdown set to "1". Below it is a "Rule Operator" section with "Logical AND of all rules". A "Profiles" section lists "ITG RiskLens Master". At the bottom of the modal are "Cancel" and "Save" buttons.

Figure 93. Setting the priority for RiskLens system views

3. Click > **Solution Configuration** > **Scheduler**.
4. Click the **RiskLens** job.
5. Click **Edit**.
6. Configure the connector:
  - Click **Client ID** and type your RiskLens client ID.
  - Click **Client Secret** and type your RiskLens client secret.
  - Verify the value in the **Api URL** and **Authentication URL** fields.
  - If you want to use other object types, click **Object Types** and type a comma-separated list of object type names.
  - In the **Schedule** section, click **Edit**. Set the schedule for the import from RiskLens.
7. Click **Done**.
 

The connector is configured and the import is scheduled.
8. To set up a risk object for assessment in RiskLens, do the following steps:
  - a) Switch to the **ITG RiskLens Master** profile.
  - b) Create a new risk.
  - c) Set **Perform Risk Analysis** to **Yes**.

The **Request Status** displays **Awaiting Submission**.

The screenshot shows a configuration panel for "RiskLens Integration". It includes a title "RiskLens Integration" with an info icon. Below the title are two sections: "Perform Risk Analysis" (set to "Yes") and "Request Status" (set to "Awaiting Submission").

Figure 94. Setting the priority for RiskLens system views

- d) Run the RiskLens job in the **Scheduler**.
- The **Request Status** displays **Awaiting Assessment**.

9. Set up RiskLens:

- a) Log in to RiskLens and click **Risk Assessment**.  
The risk that you created in step “8” on page 883 is displayed in the list.
- b) Click the risk object, then click **... > Edit Analysis Scope**.
- c) Add one or more scenarios. For more information, see the RiskLens documentation.
- d) Click **Set Scope**.
- e) Click **Run Analysis** to run the Monte Carlo simulation to generate the loss exposure metrics.
- f) When the simulation is complete, click **... > Set as Current**.
- g) In OpenPages, run the RiskLens job in the **Scheduler**.
- h) In OpenPages, go to the risk that you created in step “8” on page 883.

The view is now populated with the loss exposure metrics from RiskLens.

The screenshot shows the IBM OpenPages with Watson interface with the 'Risks' tab selected. A specific risk object, 'IT05\_RIS\_0000002', is displayed. The 'General' tab shows the risk's name, description, and status. The 'RiskLens Integration' tab shows the risk assessment configuration and its status. A red box highlights the 'Loss Exposure' section at the bottom, which provides detailed financial metrics. A modal window titled 'Risk Approved' is open on the right, indicating that the risk has been approved and is now read-only.

Figure 95. Setting the priority for RiskLens system views

Any updates to the Risk Assessment in RiskLens are pulled into OpenPages by the scheduled job if status of the Risk Assessment in RiskLens is **Current**.

# Chapter 36. IBM OpenPages Model Risk Governance

The IBM OpenPages Model Risk Governance (MRG) solution supports organizations in organizing and centralizing their model inventory.

AI Factsheets integrates with OpenPages to enable enterprises to easily document key AI technology characteristics to facilitate risk assessments and validation, enabling end-to-end automated AI Governance.

The integration allows AI Factsheets and OpenPages to exchange model information to aid in the model lifecycle. Model risk teams and model validators can use the information from AI Factsheets to aid in the risk assessment and model validation processes.

To use the integration, you need:

- IBM OpenPages for IBM Cloud Pak for Data
- AI Factsheets on IBM Cloud Pak for Data

AI Factsheets supports integration with a single OpenPages instance.

To set up the integration with AI Factsheets, do the following tasks:

- In AI Factsheets, configure the integration with your OpenPages instance. For more information, see [Integrating Factsheets with IBM OpenPages](#).
- In OpenPages:
  - Load the integration files
  - Configure the integration

## Loading the integration files for AI Factsheets

If you want to use IBM OpenPages Model Risk Governance with AI Factsheets, load the integration files.

### Before you begin

To enable the data exchange between AI Factsheets and OpenPages, the following requirements must be met:

- AI Factsheets is running in IBM Cloud Pak for Data 4.5 or later
- A standalone RabbitMQ server, if running OpenPages on-prem or on-cloud
- OpenPages running on IBM Cloud Pak for Data 4.5 or later or OpenPages on-prem or on-cloud

### About this task

The loader file for the AI Factsheets integration contains a new profile, fields, views, and other settings.

### Procedure

1. Locate the MRG folder in the IBM OpenPages General package that you downloaded from the IBM Cloud Pak for Data install media or Passport Advantage.

Alternatively, you can run the following command on the Red Hat OpenShift cluster, where OpenPages is installed, to copy the file locally:

```
oc cp openpages-<instance_name>-sts-0:/opt/ibm/OpenPages/MRG-AIFactsheets-setup-op-config.xml.zip ./MRG-AIFactsheets-setup-op-config.xml.zip
```

2. Locate the MRG-AIFactsheets-Setup-op-config.xml.zip file.

Move the file into a new directory named `mrg_files`.

3. Expand the MRG-AIFactsheets-Setup-op-config.xml.zip file in the `mrg_files` directory.
4. Locate the `MRG-AIFactsheets-Setup-op-config.xml` file.
5. Log in to OpenPages as an administrator.
6. Click  > **System Migration** > **Import Configuration**.
7. Click **Local Drive**
8. Click **Add File** and select the `MRG-AIFactsheets-Setup-op-config.xml` file.
9. Click **Import** and wait for the file to load successfully.

## What to do next

Configure the integration. See [“Configuring the AI Factsheets integration” on page 886](#).

# Configuring the AI Factsheets integration

---

You need to do some steps to configure the integration of IBM OpenPages for IBM Cloud Pak for Data and AI Factsheets.

Do this configuration after you load the integration files.

Do the following tasks:

- If you are running an on-prem or on-cloud installation of OpenPages, you must set up OpenPages to connect to a separate RabbitMQ server to exchange messages with AI Factsheets. For more information, see [“Setting up OpenPages to connect to RabbitMQ” on page 889](#).
- Assign the **MRG AI Factsheets Master** profile to users. See [“Profile” on page 886](#).
- Set up a user to give AI Factsheets access to the OpenPages API. See [“API user” on page 886](#).
- Set up the messaging from OpenPages to AI Factsheets. See [“RabbitMQ messaging” on page 886](#).
- Set the message expiration time for messages. See [“Adjusting the time-to-live for RabbitMQ messages” on page 888](#).

## Profile

The **MRG AI Factsheets Master** profile contains access to all the objects, views, and fields needed to use MRG together with AI Factsheets. Assign this profile to the users who want to use the AI Factsheets data in OpenPages.

## API user

AI Factsheets uses the OpenPages REST API to populate OpenPages objects with model facts and other data that is initially captured in AI Factsheets.

To access the OpenPages REST API, an API user must be created in OpenPages and configured with the necessary permissions. OpenPages comes with a role template that is called **MRG – AI Factsheets – API Access**, which has the minimum set of access required for the API to function with AI Factsheets. Use this role template when you define a role assignment for the API user. For more information, see [“Creating user accounts” on page 48](#).

Assign the **MRG AI Factsheets Master** profile to the API user to ensure the API user has access to all the required objects. For more information, see [“Associating profiles to a user” on page 223](#).

## RabbitMQ messaging

OpenPages uses RabbitMQ messaging to notify AI Factsheets about changes to OpenPages objects that need to be reflected in AI Factsheets. You can configure RabbitMQ messages for the following types of object changes (actions):

- Create

- Update
- Delete
- Associate
- Disassociate

[Table 252 on page 887](#) outlines the messages that are required for the integration with AI Factsheets.

<i>Table 252. Messaging requirements</i>					
<b>Object Type</b>	<b>Create</b>	<b>Update</b>	<b>Delete</b>	<b>Associate</b>	<b>Disassociate</b>
Model Use Case (Register)	X	X	X	X	X
Model (Model)	X	X	X	X	X
Model Deployment (Usage)			X		

To set up this messaging, you add GRC triggers for the object types and operations. To set up the triggers, you need to modify the `_trigger_config_.xml` file. The OpenPages Platform 3 profile includes access to all of the system files, including the `_trigger_config_.xml` file. Add the ready-to-use OpenPages Platform 3 profile to the list of available profiles for your administrators who manage system files. Using this profile, you have access to the  **System Configuration > System Files** menu items. For more information on modifying system files, see [Chapter 9, “System file management,” on page 145](#). The following is a sample of XML code for the triggers. Add each `<grcTrigger>` element to the `<trigger-definitions>` section of the file.

```

<grcTrigger name=<triggerName> event=<actionType> position=<position>>
 <rule class="com.ibm.openpages.api.trigger.oob.ContentTypeMatchRule">
 <attribute name="content.type" value=<objectType>/>
 </rule>
 <eventHandler
 class="com.ibm.openpages.api.trigger.oob.messaging.RabbitMQObjectChangeEventHandler">
 </eventHandler>
</grcTrigger>

```

<i>Table 253. Parameters</i>		
<b>Parameter</b>	<b>Description</b>	<b>Example</b>
<code>&lt;triggerName&gt;</code>	A name for the trigger	<code>grcTrigger name="RabbitMQ</code> event for Model creation”
<code>&lt;actionType&gt;</code>	The action for which you want a RabbitMQ message. The possible values are: <ul style="list-style-type: none"> <li>• <code>create.object</code></li> <li>• <code>update.object</code></li> <li>• <code>delete.objects</code></li> <li>• <code>associate.objects</code></li> <li>• <code>disassociate.objects</code></li> </ul>	<code>event="create.object"</code>

Table 253. Parameters (continued)

Parameter	Description	Example
<position>	<p>Position Events are generated in one of two phases of an operation, PRE or POST. Triggers are registered to listen for either one or other position. The possible values are:</p> <ul style="list-style-type: none"> <li>• PRE – Events that happen prior to the operation actually being performed by the system For example, during the creation of a GRC Object, a PRE event has all the information about the object to be created, but the system has yet to take action to create the object and persist values. PRE is required for deletes, associations, and disassociations.</li> <li>• POST - Events that happen after the operation has been performed by the system and before the transaction has been committed, allowing for further processing of additional business logic POST is required for creates and updates.</li> </ul> <p>For more information, see the <a href="#">OpenPages 8.3 trigger development guide</a>.</p>	position="POST"
<objectType>	The name of the object type you want to create messages for (i.e. Model, Register, Usage).	value="Model"

For an example of the complete content of `_trigger_config_.xml` content, see “[Sample trigger configuration for AI Factsheets](#)” on page 889.

## Adjusting the time-to-live for RabbitMQ messages

RabbitMQ allows for messages to expire after a specified amount of time, called the *time to live (TTL)* of the messages. In OpenPages, the TTL of RabbitMQ messages is controlled by the registry setting **Platform > Messaging > RabbitMQ > Message Time To Live (TTL)**. By default, the TTL is set to 172,800,000 milliseconds (2 days).

## Setting up OpenPages to connect to RabbitMQ

If you are running an on-prem or on-cloud installation of OpenPages, you must set up OpenPages to connect to a separate RabbitMQ server to exchange messages with AI Factsheets.

### Before you begin

You must have already downloaded and installed RabbitMQ before you follow the steps in this task. For more information, see [RabbitMQ download page](#).

If you intend to use RabbitMQ to enable the OpenPages integration with AI Governance or AI Factsheets, your RabbitMQ server configuration file, named `rabbitmq.conf`, must be configured with peer verification disabled. To do this, set the flag `ssl_options.fail_if_no_peer_cert` to `false`.

### Procedure

1. For OpenPages to connect to the standalone RabbitMQ instance, OpenPages must store the following RabbitMQ credentials, located on the application server in `/home/opuser/OP/OpenPages/aurora/conf/aurora.properties`. Replace `<servername>` with the name chosen at install time.

```
rabbitmq.host=<host name of RabbitMQ server>
rabbitmq.user= <username or RabbitMQ user>
rabbitmq.password=<password of RabbitMQ user>
rabbitmq.amqps.port= <port number of RabbitMQ server>
rabbitmq.updates.enabled = true
rabbitmq.updates.exchange.name=OpenPages.public.objects.<servername>
rabbitmq.updates.objects.queue.name=OpenPages.public.objects
```

**Note:** The value of `rabbitmq.updates.objects.queue.name` should be different on the AI Factsheets side.

2. If you did not configure SSL in the RabbitMQ setup, follow instructions from RabbitMQ on how to configure SSL: <https://www.rabbitmq.com/ssl.html>. Download the certificates `ca_certificate.pem` and `server_<server address>.certificate.pem` from the `rabbitmq/tls-gen/basic/result` directory.

Rename `server_<server address>.certificate.pem` to `server_certificate.pem`.

3. Upload the certificates to the OpenPages application server.

- a. Use the following command to load the CA certificate into the required keystore:

```
keytool -import -alias rabbitmq -trustcacerts -file ca_certificate.pem
-keystore /opt/ibm/java-x86_64-80/jre/lib/security/cacerts
```

- b. Enter the keystore password, and enter **yes** to trust the certificate.

- c. Use the following command to load the server certificate into the required keystore:

```
keytool -import -alias rabbitmq -trustcacerts -file server_certificate.pem -keystore
<OP_HOME>/OP/OpenPages/wlp/usr/servers/<server name>/resources/security/key.p12
-storetype PKCS12 -storepass <openpagesAdministrator password>
-noprompt
```

- d. After loading the certificate into the keystore, restart the OpenPages application with the `--clean` flag.

## Sample trigger configuration for AI Factsheets

The following sample shows the triggers for AI Factsheets in the `<trigger-definitions>` section of the `_trigger_config_.xml` file.

```
<?xml version="1.0" encoding="UTF-8"?>
<trigger-definitions>
 <grcTrigger name="RabbitMQ Event On Register Create" event="create.object" position="POST">
 <rule class="com.ibm.openpages.api.trigger.oob.ContentTypeMatchRule">
 <attribute name="content.type" value="Register"/>
 </rule>
 </grcTrigger>
</trigger-definitions>
```

```

<eventHandler
class="com.ibm.openpages.api.trigger.oob.messaging.RabbitMQObjectChangeEventHandler">
 </eventHandler>
</grcTrigger>
<grcTrigger name="RabbitMQ Event On Register Update" event="update.object" position="POST">
 <rule class="com.ibm.openpages.api.trigger.oob.ContentTypeMatchRule">
 <attribute name="content.type" value="Register"/>
 </rule>
<eventHandler
class="com.ibm.openpages.api.trigger.oob.messaging.RabbitMQObjectChangeEventHandler">
 </eventHandler>
</grcTrigger>
<grcTrigger name="RabbitMQ Event On Register Delete" event="delete.objects" position="PRE">
 <rule class="com.ibm.openpages.api.trigger.oob.ContentTypeMatchRule">
 <attribute name="content.type" value="Register"/>
 </rule>
<eventHandler
class="com.ibm.openpages.api.trigger.oob.messaging.RabbitMQObjectChangeEventHandler">
 </eventHandler>
</grcTrigger>
<grcTrigger name="RabbitMQ Event On Register Associate" event="associate.objects" position="PRE">
 <rule class="com.ibm.openpages.api.trigger.oob.ContentTypeMatchRule">
 <attribute name="content.type" value="Register"/>
 </rule>
<eventHandler
class="com.ibm.openpages.api.trigger.oob.messaging.RabbitMQObjectChangeEventHandler">
 </eventHandler>
</grcTrigger>
<grcTrigger name="RabbitMQ Event On Register Disassociate" event="disassociate.objects" position="PRE">
 <rule class="com.ibm.openpages.api.trigger.oob.ContentTypeMatchRule">
 <attribute name="content.type" value="Register"/>
 </rule>
<eventHandler
class="com.ibm.openpages.api.trigger.oob.messaging.RabbitMQObjectChangeEventHandler">
 </eventHandler>
</grcTrigger>
<grcTrigger name="RabbitMQ Event On Model Create" event="create.object" position="POST">
 <rule class="com.ibm.openpages.api.trigger.oob.ContentTypeMatchRule">
 <attribute name="content.type" value="Model"/>
 </rule>
<eventHandler
class="com.ibm.openpages.api.trigger.oob.messaging.RabbitMQObjectChangeEventHandler">
 </eventHandler>
</grcTrigger>
<grcTrigger name="RabbitMQ Event On Model Update" event="update.object" position="POST">
 <rule class="com.ibm.openpages.api.trigger.oob.ContentTypeMatchRule">
 <attribute name="content.type" value="Model"/>
 </rule>
<eventHandler
class="com.ibm.openpages.api.trigger.oob.messaging.RabbitMQObjectChangeEventHandler">
 </eventHandler>
</grcTrigger>
<grcTrigger name="RabbitMQ Event On Model Delete" event="delete.objects" position="PRE">
 <rule class="com.ibm.openpages.api.trigger.oob.ContentTypeMatchRule">
 <attribute name="content.type" value="Model"/>
 </rule>
<eventHandler
class="com.ibm.openpages.api.trigger.oob.messaging.RabbitMQObjectChangeEventHandler">
 </eventHandler>
</grcTrigger>
<grcTrigger name="RabbitMQ Event On Model Associate" event="associate.objects" position="PRE">
 <rule class="com.ibm.openpages.api.trigger.oob.ContentTypeMatchRule">
 <attribute name="content.type" value="Model"/>
 </rule>
<eventHandler
class="com.ibm.openpages.api.trigger.oob.messaging.RabbitMQObjectChangeEventHandler">
 </eventHandler>
</grcTrigger>
<grcTrigger name="RabbitMQ Event On Model Disassociate" event="disassociate.objects" position="PRE">
 <rule class="com.ibm.openpages.api.trigger.oob.ContentTypeMatchRule">
 <attribute name="content.type" value="Model"/>
 </rule>
<eventHandler
class="com.ibm.openpages.api.trigger.oob.messaging.RabbitMQObjectChangeEventHandler">
 </eventHandler>
</grcTrigger>
<grcTrigger name="RabbitMQ Event On Usage Create" event="create.object" position="POST">
 <rule class="com.ibm.openpages.api.trigger.oob.ContentTypeMatchRule">

```

```

 <attribute name="content.type" value="Usage" />
 </rule>
 <eventHandler
class="com.ibm.openpages.api.trigger.oob.messaging.RabbitMQObjectChangeEventHandler">
 </eventHandler>
 </grcTrigger>
 <grcTrigger name="RabbitMQ Event On Usage Update" event="update.object" position="POST">
 <rule class="com.ibm.openpages.api.trigger.oob.ContentTypeMatchRule">
 <attribute name="content.type" value="Usage" />
 </rule>
 <eventHandler
class="com.ibm.openpages.api.trigger.oob.messaging.RabbitMQObjectChangeEventHandler">
 </eventHandler>
 </grcTrigger>
 <grcTrigger name="RabbitMQ Event On Usage Delete" event="delete.objects" position="PRE">
 <rule class="com.ibm.openpages.api.trigger.oob.ContentTypeMatchRule">
 <attribute name="content.type" value="Usage" />
 </rule>
 <eventHandler
class="com.ibm.openpages.api.trigger.oob.messaging.RabbitMQObjectChangeEventHandler">
 </eventHandler>
 </grcTrigger>
 <grcTrigger name="RabbitMQ Event On Usage Associate" event="associate.objects"
position="PRE">
 <rule class="com.ibm.openpages.api.trigger.oob.ContentTypeMatchRule">
 <attribute name="content.type" value="Usage" />
 </rule>
 <eventHandler
class="com.ibm.openpages.api.trigger.oob.messaging.RabbitMQObjectChangeEventHandler">
 </eventHandler>
 </grcTrigger>
 <grcTrigger name="RabbitMQ Event On Usage Disassociate" event="disassociate.objects"
position="PRE">
 <rule class="com.ibm.openpages.api.trigger.oob.ContentTypeMatchRule">
 <attribute name="content.type" value="Usage" />
 </rule>
 <eventHandler
class="com.ibm.openpages.api.trigger.oob.messaging.RabbitMQObjectChangeEventHandler">
 </eventHandler>
 </grcTrigger>
</trigger-definitions>
```



# Chapter 37. Configuring IBM OpenPages Regulatory Compliance Management

You can configure IBM OpenPages Regulatory Compliance Management (RCM).

For example, you can import data from Ascent Reg Tech, Reg-Track, Thomson Reuters Regulatory Intelligence, or Wolters Kluwer. You can also configure the RCM Theme Deployer.

## Ascent Connector

IBM OpenPages Regulatory Compliance Management (RCM) includes a connector for Ascent Reg Tech (Ascent).

The Ascent connector enables you to load Ascent regulatory library content directly into RCM as Mandate, Sub-Mandate, and Requirement objects.

<i>Table 254. Ascent content categorization</i>	
<b>Ascent content that is categorized as a ...</b>	<b>Is loaded as a...</b>
Section	Mandate
Rule	Sub-Mandate
Task	Requirement

During the data load, Sub-Mandates are associated to their parent Mandate objects. Also, Requirements are associated to their parent Sub-Mandate and to their grandparent Mandate through its Sub-Mandate association.

When regulators update or add content, Ascent provides updates through its feeds. The updates are then loaded into OpenPages by a scheduled job to update the regulatory library objects.

**Note:** To use the connector, you must meet the following prerequisites:

- You must have an Ascent subscription. Work with Ascent to set up a feed. For more information, contact Ascent.
- You must install the Ascent connector. For more information, contact IBM OpenPages Support.

When OpenPages imports regulatory feeds from Ascent, it does the following tasks:

- Creates an object for each new incoming Mandate, Sub-Mandate, or Requirement and adds them to your regulatory library under /Library/RCM/RegLibrary/AscentRegLibrary. The Content Source field on each object is set to Ascent. For Mandates, the field is OPSS-Mand:Content Source. For Sub-Mandates, the field is OPSS-SubMand:Content Source. For Requirements, the field is OPSS-Req:Content Source.
- Updates existing Mandates and Sub-Mandates with any incoming changes.
- If a Requirement changes, the existing requirement is replaced with a new, updated Requirement.
- If an incoming Requirement has supporting information from Ascent, the import creates Ascent Supporting Information objects and adds them as children of the Requirement.

## Configuring the Ascent connector

Configure the import of Ascent Reg Tech (Ascent) data into OpenPages.

### Before you begin

To connect to Ascent, you need all of the following items:

- Your API token and API profile ID from Ascent.

## About this task

To do this task, you need the following application permissions:

- **SOX > Administration > Ascent Feed**
- **SOX > Administration > Scheduler**

By default, OpenPages imports new data and updates since the last import. You can change this default behavior. For more information, see “[Reloading Ascent data](#)” on page 894.

## Procedure

1. Log in.
2. Click  > **Solution Configuration > Scheduler**.
3. Click the **Ascent** job.
4. Click **Edit**.
5. Configure the connector:
  - Click **API Token** and enter your Ascent API token.
  - Verify the value in the **Base URL** field.
  - To change the maximum number of days' data to import, click **Max Days to Get**.
  - Click **Profile ID** and enter your Ascent profile ID.
  - In the **Schedule** section, click **Edit**. Set the schedule for the import from Ascent.
6. Click **Done**.

The connector is configured and the import is scheduled.

7. If you want to import data from Ascent now, click the checkbox next to the **Ascent** job and then click 

## What to do next

To see the progress of an import, go to  > **Solution Configuration > Scheduler**, click the **Ascent** job, and click the **Executions** tab. Click a process to view the log.

## Reloading Ascent data

You can reload Ascent data.

By default, IBM OpenPages with Watson loads changes since the last import. You can change the default behavior.

You can use the following settings:

- **Solutions > RCM > Ascent > Load Old Feeds**

When **Load Old Feeds** is false, OpenPages imports only new data. If you're importing data for the first time, you can use **Max Days To Get** to specify the number of days to import.

When **Load Old Feeds** is true, OpenPages imports all of the data that is available, including data that was imported previously, up to the **Max Days to Get**.

- **Max Days to Get** in the Ascent job configuration in the Scheduler

This setting specifies the maximum number of days to import. This setting applies in the following cases:

- The **Load Old Feeds** setting is True.
- Or, you are importing Ascent data for the first time.

When you import a new regulator, the **Max Days to Get** setting is ignored. All of the available Mandates and Submandates for the regulator are imported.

Changes to these settings take effect the next time that you import from Ascent.

### Example: Reloading data

For example, suppose that the most recent import was 10 days ago and **Max Days to Get** is set to 30. If you want to import all data for the past 30 days, set **Load Old Feeds** to true. With this configuration, OpenPages loads data from the past 30 days, even though some of the data was loaded during the previous import.

## Thomson Reuters Connector

---

IBM OpenPages Regulatory Compliance Management (RCM) includes a connector for Thomson Reuters Regulatory Intelligence (TRRI).

The Thomson Reuters connector enables you to load regulatory event feeds from Thomson Reuters into RCM. You can set up rules to process the incoming regulatory events automatically. Rules trigger workflows that are assigned to users based on the data points in the regulatory events or in the documents that are impacted by a regulatory change. The rules help you to assign tasks to users efficiently so that they can respond to and prepare for regulatory changes.

You can also import regulatory library objects from Thomson Reuters into RCM.

When OpenPages imports regulatory events, it does the following tasks:

- Checks if there is a taxonomy change.

If a new Thomson Reuters taxonomy file is found on the SFTP server, OpenPages does the following tasks:

- Updates the RCM-TRRI-Taxonomy field group
- Sends an email to the users who are set up as TRRI Administrators.

For more information, see [“Thomson Reuters taxonomy updates” on page 901](#).

- Checks if the taxonomy mapping file has changed. If a new taxonomy mapping file is found, OpenPages uses the new mappings when it imports regulatory events. For more information about the taxonomy mapping file, see [“Mapping Thomson Reuters taxonomy values to OpenPages field values” on page 900](#).

- For regulatory events, OpenPages does the following steps:

- Creates a TRRI Regulatory Event object for each new incoming regulatory event.
- Checks the series ID of each incoming regulatory event and looks for a TRRI Regulatory Event Series object with the same series ID.

If OpenPages finds a match, OpenPages associates the regulatory event with the TRRI Regulatory Event Series.

If a TRRI Regulatory Event Series object does not exist for the series ID, OpenPages creates one and associates the regulatory event with the new TRRI Regulatory Event Series object.

- Checks each of the incoming regulatory events for related documents. If the citation field on a regulatory event matches the citation field on a Mandate, Sub-Mandate, or Requirement in your regulatory library, OpenPages adds the Mandate, Sub-Mandate, or Requirement as a related object of the TRRI Regulatory Event.
- Checks each of the incoming regulatory events against all rules that are enabled in the **TRRI Rules Engine**. If the regulatory event meets all the conditions of a rule, the rule is triggered. For more information, see [“Processing regulatory events by using rules” on page 911](#).

- For regulatory library objects, OpenPages does the following steps:

- Creates an object for each new incoming Sub-Mandate and adds them to your regulatory library under Library/RCM/RegLibrary/TRRIRegLibrary. The OPSS-SubMand:Content Source field on each object is set to Thomson Reuters
- Uses the Thomson Reuters API to identify Mandates that are associated with the incoming Sub-Mandates and creates the Mandate objects in OpenPages. The new Mandates are added to your regulatory library under Library/RCM/RegLibrary/TRRIRegLibrary. The Sub-Mandates are associated with their parent Mandate. In addition, the Thomson Reuters categorizations of the Sub-Mandates are rolled up to the parent Mandate and are included in the Mandate details.
- Updates existing Sub-Mandates with any incoming changes.
- Updates existing Mandates with any new Sub-Mandate associations and any new categorizations from the associated Sub-Mandates.
- Sends an email to the owner of the impacted Sub-Mandates.

## Preparing the SFTP server

Prepare the SFTP server where the Thomson Reuters data will be delivered.

### Procedure

1. Create a directory to use with OpenPages. Or, choose an existing directory.

This is the directory where the feeds will be delivered. OpenPages will download the feeds from this directory.

2. Create a user for OpenPages on the SFTP server. Give the user read and write permissions on the directory where the feeds will be delivered.

The user needs Write permission because OpenPages creates a temporary file on the SFTP server in order to read the server's time. This file is used to keep track of which files are new and which are old, so that old files are not re-imported. OpenPages does not modify or delete existing files on the SFTP server.

3. Gather information.

You need the following information when you configure the Thomson Reuters import in OpenPages:

- The fully qualified domain name (FQDN) or IP address of the SFTP server

**Note:** Depending on your network configuration, you might need to use the IP address instead of the FQDN.

- The username and password of the user that you created in step 2
- The port number of the SFTP server (the default port is 22)
- The directory where the Thomson Reuters feeds will be delivered

This is the directory that you created in step 1.

4. Make sure that all application servers (admin and non-admin) can connect to the SFTP server by using the information in step 3.

**Tip:** You do not need to sync the clock between the OpenPages application servers and the SFTP server.

## Configuring the feeds

In Thomson Reuters Regulatory Intelligence (TRRI), choose the feeds that you want to import into IBM OpenPages with Watson.

### About this task

You can import data from multiple feeds, but the feeds must be delivered to the same directory on the SFTP server.

## Procedure

1. Set up Thomson Reuters Regulatory Intelligence to deliver feeds to the SFTP server that you prepared for OpenPages.

For more information, see “[Preparing the SFTP server](#)” on page 896.

For information about setting up Thomson Reuters Regulatory Intelligence, see the documentation that is provided with Thomson Reuters Regulatory Intelligence or contact your Thomson Reuters representative.

2. Choose the feeds that you want to import into OpenPages.

- For each feed, use the same delivery location. OpenPages reads from only one SFTP server directory.
- Enable the **Regulatory Event summaries only** option for each feed. OpenPages does not process source documents from Thomson Reuters Regulatory Intelligence.

3. Click **Settings > Taxonomy**, and then do the following steps:

- a) Set the delivery location of the taxonomies to the same directory as the feeds that you set up in step 2.
  - b) Enable the **Send taxonomy files as they are updated** check box.
4. Make a note of the directory where the feeds and taxonomy files will be delivered.

You need this information when you configure the Thomson Reuters import in OpenPages.

## Configuring the Thomson Reuters import

Configure the import of Thomson Reuters Regulatory Intelligence data into IBM OpenPages with Watson.

### Before you begin

- To connect to Thomson Reuters Regulatory Intelligence, you need all of the following items:
  - Your API client ID and API client secret from Thomson Reuters Regulatory Intelligence.
- Prepare the SFTP server. For more information, see “[Preparing the SFTP server](#)” on page 896.
- Configure the feeds in Thomson Reuters Regulatory Intelligence. For more information, see “[Configuring the feeds](#)” on page 896.
- Before you import, ensure that System Admin Mode is disabled. To disable System Admin Mode, click  > **Disable System Admin Mode**.

### About this task

To do this task, you need the **SOX > Administration > TRRI Feed** permission.

## Procedure

1. Log in.
2. Click  to open the Primary menu.
3. Click **Regulatory Compliance > TRRI Regulatory Events**.
4. Click .
5. Enter values in the following fields:
  - **API Client ID** and **API Client Secret**: Type the API client ID and secret that you received from Thomson Reuters.
  - **Host**: Type the fully qualified domain name (FQDN) or IP address of the SFTP server where the feeds are delivered.
  - **Username** and **Password**: Type the user name and password that is used by OpenPages to access the SFTP server.

- **Directory:** Type the directory on the SFTP server where the feeds are delivered. For more information, see “[Directory path for Thomson Reuters imports](#)” on page 898.
  - **Port:** Type the port number of the SFTP server (the default is 22).
  - **Daily Scheduled Import:** If you want to schedule the import, select a time. OpenPages imports the data each day. This field is optional.  
Select a time later than the time that your Thomson Reuters feeds are scheduled to be delivered. Keep in mind that it can take some time for the feeds to be delivered to the SFTP server.  
For more information, see “[Daily schedule for Thomson Reuters imports](#)” on page 898.
  - **TRRI Administrators:** Use this field to select the users to notify if the import has errors or if the Thomson Reuters taxonomy changes. This field is optional.
  - Select one or more of the following options:
    - **Process Regulatory Events:** Select this option to import regulatory events data.
    - **Process Regulatory Library Objects:** Select this option to import related documents.
6. Optional: If you want to customize how the Thomson Reuters taxonomy is mapped to OpenPages fields, see “[Thomson Reuters taxonomy mapping](#)” on page 899.
7. If you want to import data from Thomson Reuters now, click **Start Import**. Otherwise, click **Done**.

## What to do next

To see the progress of an import, go to  > **Solution Configuration** > **Scheduler**, click the **Thomson Reuters Regulatory Intelligence** job, and click the **Executions** tab. Click a process to view the log.

**Note:** The maximum file size for an import file is 10 GB. If a file is larger than the maximum, the file is skipped and a notification is sent to the **TRRI Administrators**.

## Directory path for Thomson Reuters imports

When you configure the import of Thomson Reuters data into IBM OpenPages with Watson you need to specify the directory on the SFTP server where the feeds are delivered.

You can use an absolute or a relative path.

The path is relative to the default directory of the SFTP user that OpenPages uses to access the SFTP server.

For example, suppose that you are using a Linux server, the default directory for OpenPages is /home/data, and the Thomson Reuters feeds are delivered to a subdirectory called feeds. You can specify the feeds directory by using either of the following paths:

- /home/data/feeds
- feeds

**Important:** If you type a leading forward slash (/), the meaning of the path is different. A leading forward slash indicates an absolute path relative to the root directory. So, in this example, /feeds is /home/feeds.

**Tip:** You can also use a period (.) to specify the user's default directory, in this example . is equivalent to /home/data.

If your SFTP server is using Microsoft Windows, use a backslash (\) when you type the path.

## Daily schedule for Thomson Reuters imports

When you configure the import of Thomson Reuters data into IBM OpenPages with Watson, you can choose the hour each day to do the import.

You can choose an hour between 00:00 and 23:00. OpenPages uses the clock of the OpenPages application servers to determine the time window.

Choose a time that is later than the time when the Thomson Reuters feeds are scheduled to be delivered. It can take some time for the Thomson Reuters data to arrive on the SFTP server.

For example, suppose that you choose 13:00. At 1PM each day, OpenPages attempts to import the data on the SFTP server. If the import fails, OpenPages continues to attempt the import until 1:59PM.

If OpenPages is shut down at the time you chose, OpenPages tries again when the servers are restarted, if the time window hasn't passed.

For example, suppose that you schedule the import for 13:00. If the OpenPages servers are shut down at 11:00AM and then restarted at 1:30PM, OpenPages imports the Thomson Reuters data at 1:30PM. If the servers are restarted after 1:59PM, however, OpenPages does not import data until the next day at 1PM.

## Reloading Thomson Reuters data

You can reload Thomson Reuters feeds.

By default, IBM OpenPages with Watson imports new feeds only. During an import, all files that existed before the previous import are ignored.

However, you can change the default behavior by changing the following setting to true: **Solutions > RCM > TRRI > Load Old Feeds**. When **Load Old Feeds** is true, OpenPages imports all of the feeds that are in the directory on the SFTP server. The change takes effect the next time that you import from Thomson Reuters:

For more information, see [Chapter 20, “Viewing the Configuration and Settings page,” on page 473](#).

## Thomson Reuters taxonomy mapping

You can map the Thomson Reuters taxonomy to field values in IBM OpenPages with Watson.

You map values by downloading, modifying, and then uploading the Thomson Reuters taxonomy mapping file. The mapping file is a CSV text file.

For example, the Thomson Reuters taxonomy includes theme names, but you might want to use different names for some or all of the themes. Suppose that the theme names that you want to use are in the RCM-Shared:Themes field. You can map the Thomson Reuters theme names to the values of the RCM-Shared:Themes field. The field that you use must be an enumerated string field. Add the RCM-Shared:Themes to the TRRI Regulatory Event object type and then modify the taxonomy mapping file.

The screenshot shows a Microsoft Excel spreadsheet titled "trri\_taxonomy\_map1.csv - Excel". The spreadsheet has columns A through I. Column A contains row numbers (1844 to 1857). Columns B and C contain field names ("Content Type" and "Themes"). Column D contains the corresponding taxonomy values. Columns F, G, and H contain mapped values. The data is as follows:

	A	B	C	D	E	F	G	H
1844	TRRI	Content Type	I7438E580A9FE11	Secondary Sources   Treatises				
1845	TRRI	Themes	IE5B7F470458211	Business Activities				
1846	TRRI	Themes	IE5C1B870458211	Business Activities   Banking		RCM-Shared	Themes	BA-B
1847	TRRI	Themes	IE5C22DA0458211	Business Activities   Banking   Commercial lending		RCM-Shared	Themes	BA-B-COMM-L
1848	TRRI	Themes	IE5C254B0458211	Business Activities   Banking   Consumer credit		RCM-Shared	Themes	BA-B-CON-CR
1849	TRRI	Themes	IE5C2A2D0458211	Business Activities   Banking   Electronic banking / transactions		RCM-Shared	Themes	BA-B-E-TR
1850	TRRI	Themes	ISEB44230622211	Business Activities   Banking   Foreclosure		RCM-Shared	Themes	BA-B-F
1851	TRRI	Themes	IE5C2C9E0458211	Business Activities   Banking   Foreign operations		RCM-Shared	Themes	BA-B-FO
1852	TRRI	Themes	IE5C31800458211	Business Activities   Banking   Investment activities - Banking				
1853	TRRI	Themes	IE5C1DF80458211	Business Activities   Banking   Payment systems / negotiable instruments				
1854	TRRI	Themes	IE5C38D30458211	Business Activities   Banking   Public monies				
1855	TRRI	Themes	IE5C3B440458211	Business Activities   Banking   Real estate / mortgage lending				
1856	TRRI	Themes	IE5C40260458211	Business Activities   Banking   Repayment protection				
1857	TRRI	Themes	IE5C42970458211	Business Activities   Banking   Savings and deposits				

Figure 96. Example of mapping Thomson Reuters themes to field values in OpenPages

Notice that you do not need to map all Thomson Reuters values to field values in OpenPages. If you do not map all values in the OpenPages field to a Thomson Reuters value, however, those fields will not get values automatically when the Thomson Reuters data is imported.

You can map multiple Thomson Reuters values to the same OpenPages field value.

You can also map a single Thomson Reuters value to multiple OpenPages field values. For example, suppose that you want to map the Thomson Reuters value Business Activities | Banking to BA and Banking in OpenPages. Copy the Business Activities | Banking row. In one of the rows, type BA in column H. In the other Business Activities | Banking row, type Banking in column H.

## Mapping Thomson Reuters taxonomy values to OpenPages field values

You can map values in the Thomson Reuters taxonomy to values in IBM OpenPages with Watson. You define the mappings by editing the taxonomy mapping file.

### Before you begin

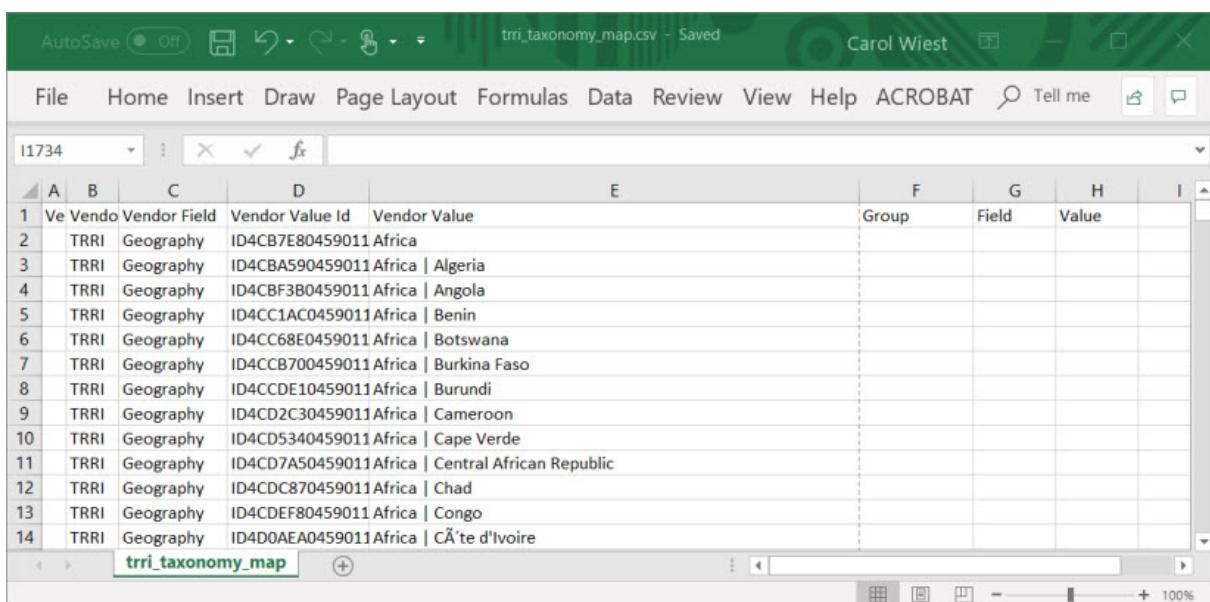
- Ensure that each field group that you want to use is associated with the TRRI Regulatory Event object type.
- Ensure that each field that you want to use is an enumerated string field. The values that you want to use in the mapping file must be available in the enumerated string field.

### About this task

To do this task, you need the **SOX > Administration > TRRI Feed** permission.

### Procedure

1. Click  to open the Primary menu.
2. Click **Regulatory Compliance > TRRI Regulatory Events**.
3. Click .
4. Click **Download the latest mapping file (.csv)** and save the file.
5. Create a backup of the `trri_taxonomy_map.csv` file.
6. Open the `trri_taxonomy_map.csv` file.



A	B	C	D	E	F	G	H	I
1	Ve Vendo Vendor Field		Vendor Value Id	Vendor Value				
2	TRRI Geography		ID4CB7E80459011	Africa				
3	TRRI Geography		ID4CBA590459011	Africa   Algeria				
4	TRRI Geography		ID4CBF3B0459011	Africa   Angola				
5	TRRI Geography		ID4CC1AC0459011	Africa   Benin				
6	TRRI Geography		ID4CC68E0459011	Africa   Botswana				
7	TRRI Geography		ID4CCB700459011	Africa   Burkina Faso				
8	TRRI Geography		ID4CCDE10459011	Africa   Burundi				
9	TRRI Geography		ID4CD2C30459011	Africa   Cameroon				
10	TRRI Geography		ID4CD5340459011	Africa   Cape Verde				
11	TRRI Geography		ID4CD7A50459011	Africa   Central African Republic				
12	TRRI Geography		ID4CDC870459011	Africa   Chad				
13	TRRI Geography		ID4CDEF80459011	Africa   Congo				
14	TRRI Geography		ID4D0AE0459011	Africa   Côte d'Ivoire				

Figure 97. Example of the taxonomy file in Microsoft Excel

7. In column E, locate the Thomson Reuters value that you want to map to a field value in OpenPages.

8. For each value that you want to map, enter the following information:

- In column F, type the field group.
- In column G, type the field name.
- In column H, type the field value.

The Thomson Reuters value in column E will be mapped to the OpenPages value in column H.

**Note:** Do not edit the values in columns A to E.

9. Save the file as a CSV text file.

10. Return to OpenPages.

11. On the **TRRI Regulatory Events** page, click .

12. Click **Upload**.

## Results

The taxonomy mapping file is uploaded. The next time that you import data from Thomson Reuters, your taxonomy mappings are applied to the incoming regulatory events.

## Thomson Reuters taxonomy updates

If you modified the taxonomy mapping file, you need to update it when the Thomson Reuters taxonomy changes.

When Thomson Reuters updates the taxonomy, it delivers a new taxonomy file to the SFTP server. IBM OpenPages with Watson checks for a new taxonomy file each time it imports data from Thomson Reuters. If OpenPages detects a new taxonomy file, it updates the fields in the RCM - TRRI - Taxonomy field group and then sends an email to the **TRRI Administrators**. The **TRRI Administrators** are configured when you configure the Thomson Reuters import. For more information, see [“Configuring the Thomson Reuters import” on page 897](#).

Review the taxonomy changes that are listed in the email. Download the taxonomy mapping file, locate the new taxonomy values, and update the mappings. You might also need to update the fields in OpenPages. For example, if Thomson Reuters adds a new theme to the taxonomy, you might need to add a new value to the field that you use for theme names. When the taxonomy mapping file is ready and the OpenPages fields are updated, upload the taxonomy mapping file. For more information, see [“Mapping Thomson Reuters taxonomy values to OpenPages field values” on page 900](#).

## Reg-Track connector

IBM OpenPages Regulatory Compliance Management (RCM) includes a connector for Reg-Track.

The Reg-Track connector enables you to load regulatory events from Reg-Track into RCM. You can set up rules to process the incoming regulatory events automatically. Rules trigger workflows that are assigned to users based on the data points in the regulatory events. The rules help you to assign tasks to users efficiently so that they can respond to and prepare for regulatory changes.

**Note:** To use the connector, you must meet the following prerequisites:

- You must have a Reg-Track subscription. For more information, contact Reg-Track.
- You must install the Reg-Track connector. For more information, contact your IBM representative.

When OpenPages imports regulatory event feeds from Reg-Track, it does the following tasks:

- Checks if there are any changes to the Reg-Track taxonomy.

If changes are found, OpenPages does the following tasks:

- Updates the fields in the RCM-RegTrack-Taxonomy field group.
- Sends an email to the users who are set up as Reg-Track Administrators.

For more information, see [“Reg-Track taxonomy updates” on page 905](#).

- Checks if the taxonomy mapping file has changed. If a new taxonomy mapping file is found, OpenPages uses the new mappings when it imports regulatory feeds. For more information about the taxonomy mapping file, see “[Mapping Reg-Track taxonomy values to OpenPages field values](#)” on page 904.
- For regulatory events, OpenPages does the following steps:
  - Creates a Reg-Track Regulatory Event object for each new incoming regulatory event.
  - Checks the Reg-Track Series ID of each incoming regulatory event and looks for a Reg-Track Regulatory Event Series object with the same series ID.

If OpenPages finds a match, OpenPages associates the regulatory event with the Reg-Track Regulatory Event Series.

If a Reg-Track Regulatory Event Series object does not exist for the series ID, OpenPages creates one and associates the regulatory event with the new Reg-Track Regulatory Event Series object.

  - Checks each of the incoming regulatory events against all of the Reg-Track rules that are enabled in OpenPages. If the regulatory event meets the conditions of a rule, the rule is triggered. For more information, see “[Processing regulatory events by using rules](#)” on page 911.

## Configuring the Reg-Track connector

Configure the import of Reg-Track data into OpenPages.

### Before you begin

To connect to Reg-Track, you need all of the following items:

- The Reg-Track API URL.
- Your Reg-Track API client key.
- Your Reg-Track API client secret.
- Your Reg-Track API token.

Before you import, ensure that System Admin Mode is disabled. To disable System Admin Mode, click  > **Disable System Admin Mode**.

### About this task

To do this task, you need the **SOX > Administration > RegTrack Feed** application permission.

By default, OpenPages imports new data and updates since the last import. You can change this default behavior. For more information, see “[Data import settings for Reg-Track feeds](#)” on page 903.

**Note:** When you run the import for the first time, OpenPages imports data for the past 7 days by default.

### Procedure

1. Click  to open the Primary menu.
2. Click **Regulatory Compliance > Reg-Track Regulatory Events**.
3. Click .
4. Configure the import:
  - Type the API parameters that were provided to you by Reg-Track.
  - **Daily Scheduled Import:** If you want to schedule the import, select a time. OpenPages imports the data each day. This field is optional.  
Select a time that is later than when Reg-Track delivers its feeds. Contact Reg-Track for information about when feeds are delivered.
  - **Reg-Track Administrators:** Use this field to select the users to notify if the import has errors or if the Reg-Track taxonomy changes. This field is optional.

- **Process Regulatory Events:** Click to map incoming regulatory events to Reg-Track Regulatory Events in OpenPages. If not selected, OpenPages checks for an updated taxonomy file only.
5. Optional: If you want to customize how the Reg-Track taxonomy is mapped to OpenPages fields, see “Reg-Track taxonomy mapping” on page 903.
  6. If you want to import data from Reg-Track now, click **Start Import**. Otherwise, click **Done**.

## What to do next

To see the progress of an import, go to  > **Solution Configuration** > **Scheduler**, click the **Reg Track** job, and click the **Executions** tab. Click a process to view the log.

## Data import settings for Reg-Track feeds

By default, OpenPages imports new data only. You can change this default behavior.

You can use the following settings:

- **Solutions > RCM > RegTrack > Load Old Feeds**

When **Load Old Feeds** is false, OpenPages imports only new data. The maximum number of days to import is specified in the **Max Days To Get** setting.

When **Load Old Feeds** is true, OpenPages loads the data from previous days, regardless of whether the data was imported previously. You can import data from a maximum of 7 days ago. The maximum number of days to import is specified in the **Max Days To Get** setting.

- **Solutions > RCM > RegTrack > Max Days To Get**

This setting specifies the maximum number of days to import. The default value is 5. The maximum number of days that you can import is 7.

Changes to these settings take effect the next time that you import from Reg-Track.

For more information, see [Chapter 20, “Viewing the Configuration and Settings page,” on page 473](#).

### Example 1: Setting the maximum number of days of new data to import

Suppose you want to load any new data from the past 5 days.

In this case, set **Load Old Feeds** to false and set **Max Days To Get** to 5. With this configuration, OpenPages loads new data up to a maximum of 5 days ago. If the most recent import occurred 2 days ago, OpenPages loads the data only for the last 2 days. If the most recent import occurred 4 days ago, OpenPages loads the data only for the last 4 days.

### Example 2: Reloading data

Suppose that the most recent import was 3 days ago but you want to get all data from the past 7 days.

In this case, set **Load Old Feeds** to true and set **Max Days To Get** to 7. With this configuration, OpenPages loads data from the past 7 days, even though some of the data was loaded during the previous import.

## Reg-Track taxonomy mapping

You can map the Reg-Track taxonomy to field values in IBM OpenPages with Watson.

You map values by downloading, modifying, and then uploading the Reg-Track taxonomy mapping file. The mapping file is a CSV text file.

For example, the Reg-Track taxonomy includes countries and regions. You might want to group the countries into different regions or create additional regions. Suppose that the values that you want to use are in the RCM-Shared:CustomGeo field. You can map the Reg-Track countries to the values of the RCM-Shared:CustomGeo field. The field that you use must be an enumerated string field. Add

the RCM-Shared:CustomGeo field to the Reg-Track Regulatory Event object type and then modify the taxonomy mapping file.

**Note:** The following figure shows a excerpt of rows from the taxonomy mapping file to illustrate the example. This figure is not a representation of the entire file.

A	B	C	D	E	F	G	H	
3	Version	Vendor	Vendor Field	Vendor Value Id	Vendor Value	Group	Field	Value
4	Reg-Track	Countries		118	Antigua	RCM-Shared	CustomGeo	Caribbean
5	Reg-Track	Countries		121	Aruba	RCM-Shared	CustomGeo	Caribbean
6	Reg-Track	Countries		79	Bahamas	RCM-Shared	CustomGeo	Caribbean
7	Reg-Track	Countries		75	Cayman Islands	RCM-Shared	CustomGeo	Caribbean
8	Reg-Track	Countries		181	Jamaica	RCM-Shared	CustomGeo	Caribbean
9	Reg-Track	Countries		153	Trinidad and Tobago	RCM-Shared	CustomGeo	Caribbean
10	Reg-Track	Countries		150	US Virgin Islands	RCM-Shared	CustomGeo	Caribbean
11	Reg-Track	Countries		36	Yemen			
12	Reg-Track	Countries		59	Zimbabwe			

Figure 98. Example of mapping Reg-Track countries to a field value in OpenPages

You do not need to map all Reg-Track values to field values in OpenPages. If you do not map all values in the OpenPages fields to a Reg-Track value, those fields will not get values automatically when the Reg-Track data is imported.

You can map multiple Reg-Track values to the same OpenPages field value.

You can also map a single Reg-Track value to multiple OpenPages field values. For example, suppose that you want to map the Reg-Track value ABS to Derivatives and Asset Backed Securities in OpenPages. Copy the ABS row. In one of the rows, type Derivatives in column H. In the other ABS row, type Asset Backed Securities in column H.

## Mapping Reg-Track taxonomy values to OpenPages field values

You can map values in the Reg-Track taxonomy to values in IBM OpenPages with Watson. You define the mappings by editing the taxonomy mapping file.

### Before you begin

- Each field group that you want to use is associated with the Reg-Track Regulatory Event object type.
- Each field that you want to use is an enumerated string field. The values that you want to use in the mapping file must be available in the enumerated string field.

### About this task

To do this task, you need the **SOX > Administration > RegTrack Feed** permission.

When you edit the taxonomy mapping file, use a text editor that supports UTF-8. Multibyte characters are not supported in the taxonomy mapping file.

### Procedure

1. Click to open the Primary menu.

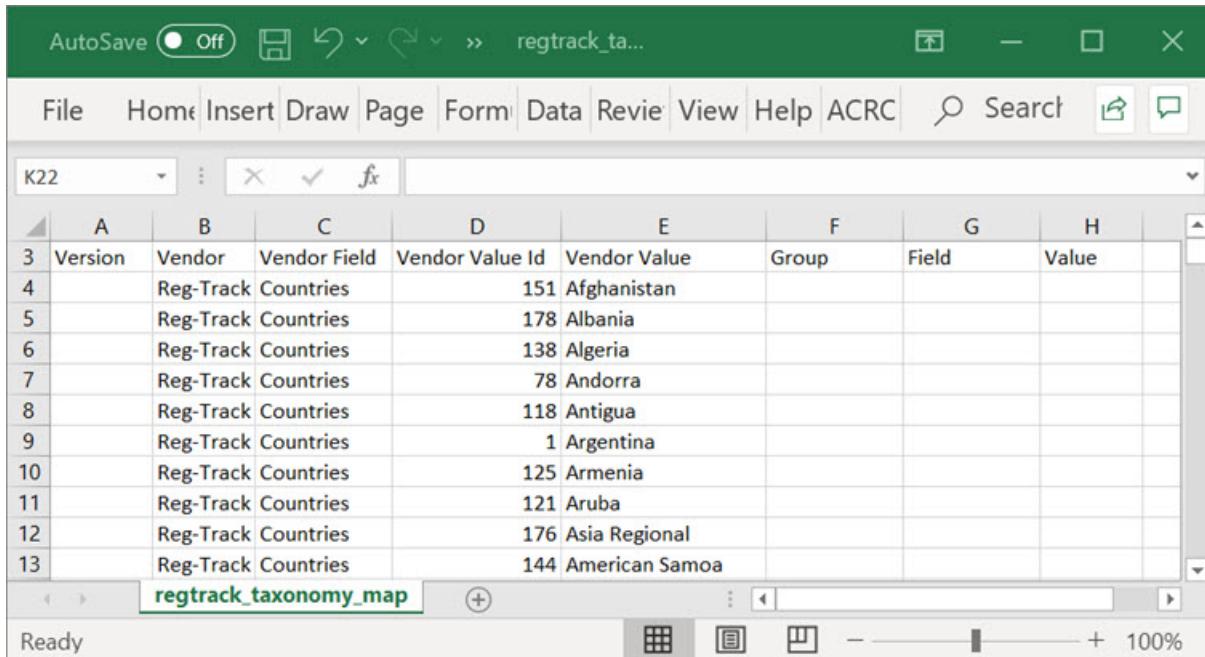
2. Click **Regulatory Compliance > Reg-Track Regulatory Events**.

3. Click .

4. Click **Download the latest mapping file (.csv)** and save the file.

5. Create a backup of the `regtrack_taxonomy_map.csv` file.

6. Open the `regtrack_taxonomy_map.csv` file.



	A	B	C	D	E	F	G	H
3	Version	Vendor	Vendor Field	Vendor Value Id	Vendor Value	Group	Field	Value
4		Reg-Track	Countries		151	Afghanistan		
5		Reg-Track	Countries		178	Albania		
6		Reg-Track	Countries		138	Algeria		
7		Reg-Track	Countries		78	Andorra		
8		Reg-Track	Countries		118	Antigua		
9		Reg-Track	Countries		1	Argentina		
10		Reg-Track	Countries		125	Armenia		
11		Reg-Track	Countries		121	Aruba		
12		Reg-Track	Countries		176	Asia Regional		
13		Reg-Track	Countries		144	American Samoa		

Figure 99. Example of the taxonomy file in Microsoft Excel

7. In column E, locate the Reg-Track value that you want to map to a field value in OpenPages.

8. For each value that you want to map, enter the following information:

- In column F, type the field group.
- In column G, type the field name.
- In column H, type the field value.

The Reg-Track value in column E will be mapped to the value in column H.

**Note:** Do not edit the values in columns A to E.

9. Save the file as a CSV text file.

10. Return to OpenPages.

11. On the **Reg-Track Regulatory Events** page, click .

12. Click **Upload**.

## Results

The taxonomy mapping file is uploaded. The next time that you import data from Reg-Track, your taxonomy mappings are applied to the incoming regulatory events.

## Reg-Track taxonomy updates

If you modified the taxonomy mapping file, you need to update it when the Reg-Track taxonomy changes.

IBM OpenPages with Watson checks for taxonomy changes each time it imports data from Reg-Track.

If OpenPages detects changes to the taxonomy, it updates the fields in the RCM-RegTrack-Taxonomy field group and then sends an email to the **Reg-Track Administrators**. The **Reg-Track Administrators** are configured when you configure the Reg-Track connector. For more information, see “[Configuring the Reg-Track connector](#)” on page 902.

Review the taxonomy changes that are listed in the email. Download the taxonomy mapping file, locate the new taxonomy values, and update the mappings. You might also need to update the fields in OpenPages. For example, if Reg-Track adds a new product type to the taxonomy, you might need to add a new value to the field that you use for product types. When the taxonomy mapping file is ready and the OpenPages fields are updated, upload the taxonomy mapping file. For more information, see “[Mapping Reg-Track taxonomy values to OpenPages field values](#)” on page 904.

## Wolters Kluwer Connector

---

IBM OpenPages Regulatory Compliance Management (RCM) includes a connector for Wolters Kluwer (WK).

The Wolters Kluwer connector enables you to load regulatory feeds from Wolters Kluwer into RCM. You can set up rules to process the incoming regulatory data automatically. Rules trigger workflows that are assigned to users based on the data points in the regulatory events or in the documents that are impacted by a regulatory change. The rules help you to assign tasks to users efficiently so that they can respond to and prepare for regulatory changes.

**Note:** To use the connector, you must meet the following prerequisites:

- You must have a Wolters Kluwer license. For more information, contact Wolters Kluwer.
- You must install the Wolters Kluwer connector. For more information, contact IBM OpenPages Support.

When OpenPages imports regulatory feeds from Wolters Kluwer, it does the following tasks:

- Checks if there are any changes to the Wolters Kluwer taxonomy.

If changes are found, OpenPages does the following tasks:

- Updates the fields in the RCM-WK-Taxonomy field group.
- Sends an email to the users who are set up as Wolters Kluwer Administrators.

For more information, see “[Wolters Kluwer taxonomy updates](#)” on page 910.

- Checks if the taxonomy mapping file has changed. If a new taxonomy mapping file is found, OpenPages uses the new mappings when it imports regulatory feeds. For more information about the taxonomy mapping file, see “[Mapping Wolters Kluwer taxonomy values to OpenPages field values](#)” on page 909.
- For regulatory events, OpenPages does the following steps:
  - Creates a WK Regulatory Event object for each new incoming regulatory event.
  - Checks each of the incoming regulatory events for related documents in your regulatory library. If the citation field on a regulatory event matches the citation field on a Mandate, Sub-Mandate, or Requirement, OpenPages adds the Mandate, Sub-Mandate, or Requirement as a related object of the WK Regulatory Event.
  - Checks each of the incoming regulatory events against all of the Wolters Kluwer rules that are enabled in OpenPages. If the regulatory event meets the conditions of a rule, the rule is triggered. For more information, see “[Processing regulatory events by using rules](#)” on page 911.
- For regulatory library objects, OpenPages does the following steps:
  - Creates an object for each new incoming Mandate or Sub-Mandate and adds them to your regulatory library under Library/RCM/RegLibrary/WKRegLibrary. The Content Source field on each object is set to Wolters Kluwer. For Mandates, the field is OPSS-Mand:Content Source. For Sub-Mandates, the field is OPSS-SubMand:Content Source.
  - Updates existing Mandates and Sub-Mandates with any incoming changes.
  - Sends an email to the owner of the impacted Mandates and Sub-Mandates.

# Configuring the Wolters Kluwer import

Configure the import of Wolters Kluwer data into IBM OpenPages with Watson.

## Before you begin

To connect to Wolters Kluwer, get the following URLs and Feed Manager API parameters from Wolters Kluwer:

- The authentication URL for the Wolters Kluwer API
- The API URL for regulatory change updates.
- The API URL for regulatory library updates.
- Your Wolters Kluwer Client ID.
- Your Wolters Kluwer Client Secret.
- Your username and password for the Wolters Kluwer API.
- The docSourceName parameter.
- The sourceSystemCode parameter.
- The transformCode parameter.

Before you import, ensure that System Admin Mode is disabled. To disable System Admin Mode, click  > **Disable System Admin Mode**.

## About this task

To do this task, you need the **SOX > Administration > WK Feed** application permission.

By default, OpenPages imports new data only, and only for the past five days. You can change this default behavior. For more information, see [“Data import settings for Wolters Kluwer feeds” on page 908](#).

## Procedure

1. Click  to open the Primary menu.
2. Click **Regulatory Compliance > WK Regulatory Events**.
3. Click .
4. Configure the import:
  - Type the URLs and API parameters that were provided to you by Wolters Kluwer.
  - **Daily Scheduled Import:** If you want to schedule the import, select a time. OpenPages imports the data each day. This field is optional.  
Select a time that is later than when Wolters Kluwer delivers its feeds. Contact Wolters Kluwer for information about when feeds are delivered.
  - **Wolters Kluwer Administrators:** Use this field to select the users to notify if the import has errors or if the Wolters Kluwer taxonomy changes. This field is optional.
  - **Process Regulatory Events:** Click to map Wolters Kluwer regulatory events to WK Regulatory Events in OpenPages..
  - **Process Regulatory Library Objects:** Click to map Wolters Kluwer library objects to Mandates, Sub-Mandates, and Requirements in OpenPages.
5. Optional: If you want to customize how the Wolters Kluwer taxonomy is mapped to OpenPages fields, see [“Wolters Kluwer taxonomy mapping” on page 908](#).
6. If you want to import data from Wolters Kluwer now, click **Start Import**. Otherwise, click **Done**.

## What to do next

To see the progress of an import, go to  > **Solution Configuration** > **Scheduler**. click the **Wolters Kluwer** job, and click the **Executions** tab. Click a process to view the log.

## Data import settings for Wolters Kluwer feeds

By default, OpenPages imports new data only, and only for the past 5 days. You can change this default behavior.

You can use the following settings:

- **Solutions > RCM > WK > Load Old Feeds**

When **Load Old Feeds** is false, OpenPages imports only new data. If you're importing data for the first time, you can use **Max Days To Get** to specify the number of days to import.

When **Load Old Feeds** is true, OpenPages loads the data from previous days, regardless of whether the data was imported previously. The maximum number of days to import is specified in the **Max Days To Get** setting.

- **Solutions > RCM > WK > Max Days To Get**

This setting specifies the maximum number of days to import. The default value is 5. This setting applies in the following cases:

- The **Load Old Feeds** setting is True.
- Or, you are importing Wolters Kluwer data for the first time.

Changes to these settings take effect the next time that you import from Wolters Kluwer.

For more information, see [Chapter 20, “Viewing the Configuration and Settings page,” on page 473](#).

## Example: Reloading data

Suppose that the most recent import was 5 days ago but you want to get all data from the past 10 days.

In this case, set **Load Old Feeds** to true and set **Max Days To Get** to 10. With this configuration, OpenPages loads data from the past 10 days, even though some of the data was loaded during the previous import.

## Wolters Kluwer taxonomy mapping

You can map the Wolters Kluwer taxonomy to field values in IBM OpenPages with Watson.

You map values by downloading, modifying, and then uploading the Wolters Kluwer taxonomy mapping file. The mapping file is a CSV text file.

For example, the Wolters Kluwer taxonomy includes jurisdictions, but you might want to use different groupings for some or all of the jurisdictions. Suppose that the values that you want to use are in the RCM-Shared:CustomGeo field. You can map the Wolters Kluwer jurisdictions to the values of the RCM-Shared:CustomGeo field. The field that you use must be an enumerated string field. Add the RCM-Shared:CustomGeo field to the WK Regulatory Event object type and then modify the taxonomy mapping file.

	A	B	C	D	E	F	G	H	I
8	WK	Jurisdiction	WKFS-JUR-0000233	Eastern Asia   South Korea   Nepal					
9	WK	Jurisdiction	WKFS-JUR-0000234	Eastern Asia   South Korea   Pakistan					
10	WK	Jurisdiction	WKFS-JUR-0000235	Eastern Asia   South Korea   Sri Lanka					
11	WK	Jurisdiction	WKFS-JUR-0000279	North America   Canada   Alberta	RCM-Shared	CustomGeo	Canada-West		
12	WK	Jurisdiction	WKFS-JUR-0000280	North America   Canada   British Columbia	RCM-Shared	CustomGeo	Canada-West		
13	WK	Jurisdiction	WKFS-JUR-0000281	North America   Canada   Manitoba	RCM-Shared	CustomGeo	Canada-West		
14	WK	Jurisdiction	WKFS-JUR-0000283	North America   Canada   New Brunswick					
15	WK	Jurisdiction	WKFS-JUR-0000282	North America   Canada   Newfoundland & Labrador					
16	WK	Jurisdiction	WKFS-JUR-0000284	North America   Canada   Northwest Territories					
17	WK	Jurisdiction	WKFS-JUR-0000291	North America   Canada   Nova Scotia					
18	WK	Jurisdiction	WKFS-JUR-0000285	North America   Canada   Nunavut					
19	WK	Jurisdiction	WKFS-JUR-0000286	North America   Canada   Ontario					
20	WK	Jurisdiction	WKFS-JUR-0000287	North America   Canada   Prince Edward Island					

Figure 100. Example of mapping Wolters Kluwer jurisdictions to field values in OpenPages

Notice that you do not need to map all Wolters Kluwer values to field values in OpenPages. If you do not map all values in the OpenPages fields to a Wolters Kluwer value, those fields will not get values automatically when the Wolters Kluwer data is imported.

You can map multiple Wolters Kluwer values to the same OpenPages field value.

You can also map a single Wolters Kluwer value to multiple OpenPages field values. For example, suppose that you want to map the Wolters Kluwer value Audit Practice Bulletins to Audit Practices and Bulletins in OpenPages. Copy the Audit Practice Bulletins row. In one of the rows, type Audit Practices in column H. In the other Audit Practice Bulletins row, type Bulletins in column H.

## Mapping Wolters Kluwer taxonomy values to OpenPages field values

You can map values in the Wolters Kluwer taxonomy to values in IBM OpenPages with Watson. You define the mappings by editing the taxonomy mapping file.

### Before you begin

- Each field group that you want to use is associated with the WK Regulatory Event object type.
- Each field that you want to use is an enumerated string field. The values that you want to use in the mapping file must be available in the enumerated string field.

### About this task

To do this task, you need the **SOX > Administration > WK Feed** permission.

When you edit the taxonomy mapping file, use a text editor that supports UTF-8. Multibyte characters are not supported in the taxonomy mapping file.

### Procedure

1. Click  to open the Primary menu.
2. Click **Regulatory Compliance > WK Regulatory Events**.
3. Click .

4. Click **Download the latest mapping file (.csv)** and save the file.
5. Create a backup of the `wk_taxonomy_map.csv` file.
6. Open the `wk_taxonomy_map.csv` file.

1	Versi	Vend	Vendor Field	Vendor Value Id	Vendor Value	Group	Field	Value
2	WK	Jurisdiction	WKFS-JUR-0000	Eastern Asia   South Korea   Afghanistan				
3	WK	Jurisdiction	WKFS-JUR-0000	Eastern Asia   South Korea   Bangladesh				
4	WK	Jurisdiction	WKFS-JUR-0000	Eastern Asia   South Korea   Bhutan				
5	WK	Jurisdiction	WKFS-JUR-0000	Eastern Asia   South Korea   India				
6	WK	Jurisdiction	WKFS-JUR-0000	Eastern Asia   South Korea   Iran (Islamic Republic of)				
7	WK	Jurisdiction	WKFS-JUR-0000	Eastern Asia   South Korea   Maldives				
8	WK	Jurisdiction	WKFS-JUR-0000	Eastern Asia   South Korea   Nepal				
9	WK	Jurisdiction	WKFS-JUR-0000	Eastern Asia   South Korea   Pakistan				
10	WK	Jurisdiction	WKFS-JUR-0000	Eastern Asia   South Korea   Sri Lanka				
11	WK	Jurisdiction	WKFS-JUR-0000	North America   Canada   Alberta				
12	WK	Jurisdiction	WKFS-JUR-0000	North America   Canada   British Columbia				
13	WK	Jurisdiction	WKFS-JUR-0000	North America   Canada   Manitoba				

Figure 101. Example of the taxonomy file in Microsoft Excel

7. In column E, locate the Wolters Kluwer value that you want to map to a field value in OpenPages.
  8. For each value that you want to map, enter the following information:
    - In column F, type the field group.
    - In column G, type the field name.
    - In column H, type the field value.
- The Wolters Kluwer value in column E will be mapped to the value in column H.
- Note:** Do not edit the values in columns A to E.
9. Save the file as a CSV text file.
  10. Return to OpenPages.
  11. On the **WK Regulatory Events** page, click .
  12. Click **Upload**.

## Results

The taxonomy mapping file is uploaded. The next time that you import data from Wolters Kluwer, your taxonomy mappings are applied to the incoming regulatory events.

## Wolters Kluwer taxonomy updates

If you modified the taxonomy mapping file, you need to update it when the Wolters Kluwer taxonomy changes.

IBM OpenPages with Watson checks for taxonomy changes each time it imports data from Wolters Kluwer. If OpenPages detects changes to the taxonomy, it updates the fields in the RCM-WK-Taxonomy field group and then sends an email to the **Wolters Kluwer Administrators**. The **Wolters Kluwer Administrators** are configured when you configure the Wolters Kluwer import. For more information, see “Configuring the Wolters Kluwer import” on page 907.

Review the taxonomy changes that are listed in the email. Download the taxonomy mapping file, locate the new taxonomy values, and update the mappings. You might also need to update the fields in OpenPages. For example, if Wolters Kluwer adds a new document type to the taxonomy, you might need to add a new value to the field that you use for document type names. When the taxonomy mapping file is ready and the OpenPages fields are updated, upload the taxonomy mapping file. For more information, see [“Mapping Wolters Kluwer taxonomy values to OpenPages field values” on page 909](#).

## Processing regulatory events by using rules

---

You can process incoming regulatory events from Thomson Reuters Regulatory Intelligence or Wolters Kluwer by using rules.

### About this task

You use rules to trigger automated workflows. An automated workflow has only two types of stages: a start stage and one or more end stages. An automated workflow progresses from one stage to another automatically, without user interaction. OpenPages provides sample automated workflows. You can also create your own. When you create a workflow, enable the **Automated** option. The workflow is then available to use in rules.

OpenPages provides sample rules, which you can use or modify to meet your requirements. The sample rules are disabled by default. You can also create your own rules.

When a regulatory event is created, it's evaluated against all the rules that are enabled. For each rule, if its conditions are met, the automated workflow that is configured in the rule is started. A regulatory event can trigger more than one rule. The assignees and criticality are passed to the workflow as process variables. The workflow can use these parameters in values or regular expressions.

**Note:** Rules in the Rules Engine are triggered only as a result of a Thomson Reuters Regulatory Intelligence or Wolters Kluwer import.

### Procedure

#### 1. Learn about rules.

For example, look at the sample rules.

#### 2. Create automated workflows to use in rules.

For more information, see [“Target actions in rules” on page 913](#).

#### 3. Create rules.

For more information, see [“Creating rules” on page 911](#).

You can also edit rules, copy rules, delete rules, and enable or disable rules.

## Creating rules

Create rules to route incoming Regulatory Events to users and groups.

### About this task

To do this task, you need the **SOX > Administration > Rules Engine** permission.

### Procedure

#### 1. Click to open the Primary menu.

#### 2. Do one of the following steps:

- If you are using Thomson Reuters Regulatory Intelligence, click **Regulatory Compliance > TRRI Regulatory Events** and then click **TRRI Rules Engine**.

- If you are using Wolters Kluwer, click **Regulatory Compliance > WK Regulatory Events** and then click **Wolters Kluwer Rules Engine**.

### 3. Click **New Rule**.

**Note:** You can also create a rule by copying an existing rule. See “[Copying a rule](#)” on page 914.

#### 4. Type a **Name** for the rule.

#### 5. Add one or more conditions.

When a regulatory event meets the conditions in a rule, the target action is triggered.

For more information, see “[Conditions in rules](#)” on page 912.

#### 6. Select a **Target Action**.

Each action in the list is an automated workflow. When the conditions of the rule are all true, the automated workflow is started.

For more information, see “[Target actions in rules](#)” on page 913.

#### 7. Select one or more **Users and Groups** to assign to the workflow.

#### 8. Optional: Select a **Criticality**.

#### 9. Click **Done**.

**Tip:** To delete a rule, click its check box and then click **Delete**. You can also disable a rule. See “[Enabling and disabling rules](#)” on page 914.

## Conditions in rules

You can add one or more conditions to a rule. For each condition you build a comparison statement with two fields and an operator.

In **Compare** you choose the first field in the comparison statement.

- **A field in the current object**

Select an **Object Field**.

- **A field in a related object**

– Select Direct Child, Direct Parent, Ancestor, or Descendant in **Relationship Type**.

– Select an object type in **Related Object Type**.

– Select a field in **Related Object Field**.

– Select a path in **Relationship Paths** (displays only if **Relationship Type** is Ancestor or Descendant).

– Add **Filter By** conditions (optional).

– Set **Primary Parent Only** (displays only if **Relationship Type** is Direct Parent or Ancestor) (optional).

- **A field in a Preference object**

Select a **Preference Object Field**. You can add **Filter By** conditions.

- **End User**

An **End User** condition checks whether the signed on end user is a specified user and whether the user is in a specified user group. The second field in the comparison statement is a specified value, an expression, or an actor field on an object.

In **Using** you choose an operator. The list of operators depends on the first field's field type.

In **To** you choose the second field in the comparison statement:

- **A specified value**

The value that you can provide depends on the field type of the field you chose in **Compare**. The comparison is case sensitive, so ensure that you specify the correct case for the value.

- **An expression**

Enter a single field or variable from the list in “[Using variables, functions, and fields](#)” on page 377. All of the variables and fields listed there can be used in an expression. The field or variable must be in the given format. It can, however, be part of a longer string, for example, a file name like Evidence\_[\$Parent:SOXRisk/System Fields:Name\$].pdf if you want to validate that the parent object has a specific PDF attachment.

- **A field in the current object**

Select an **Object Field**.

- **A field in a related object**

- Select **Direct Child**, **Direct Parent**, **Ancestor**, or **Descendant** in **Relationship Type**.
- Select an object type in **Related Object Type**.
- Select a field in **Related Object Field**.
- Select a path in **Relationship Paths** (displays only if **Relationship Type** is Ancestor or Descendant).
- Add **Filter By** conditions (optional).
- Set **Primary Parent Only** (displays only if **Relationship Type** is Direct Parent or Ancestor) (optional).

- **A field in a Preference object**

Select a **Preference Object Field**. You can add **Filter By** conditions.

**Note:** Do not use the System Comment field (System Fields:Comment) in rules. This system field is a special field that is used with File (SOXDocument) and Signature objects.

By default, all conditions must be met for the workflow in the **Target Action** field to start. However, you can override this default behavior by defining advanced logic to combine the conditions in a specific way. To override the default behavior, set **Advanced Logic** to true. Write a statement in **Logic**. Use the condition numbers together with the operators and, or, not, and parentheses. The order of operations is:

1. ( )
2. NOT
3. AND
4. OR

For example, if you define three conditions, the default logic is that the target action is triggered if all three conditions are met: 1 and 2 and 3. However, if you define advanced logic, you can use the condition numbers together with the operators and, or, not, and parentheses:

- 1 or 2 or 3
- 1 and (2 or 3)
- 1 not (2 or 3)

## Target actions in rules

When you create a rule, you specify a target action. The target action is the automated workflow that is triggered when the conditions in the rule are true.

Each target action in the **Target Action** list is an automated workflow. You can add target actions to the list by creating automated workflows.

An automated workflow has only two types of stages: a start stage and one or more end stages. An automated workflow progresses from one stage to another automatically, without user interaction. In the workflow properties, **Automated** is set to **True**. The **Send Email Notification** workflow is an example of an automated workflow. For more information about workflows, see [Chapter 16, “Configuring GRC Workflow,” on page 369](#).

## Copying a rule

You can create a rule by copying an existing rule and then changing its properties.

### About this task

To do this task, you need the **SOX > Administration > Rules Engine** permission.

### Procedure

1. Click  to open the Primary menu.
2. Do one of the following steps:
  - If you are using Thomson Reuters Regulatory Intelligence, click **Regulatory Compliance > TRRI Regulatory Events** and then click **TRRI Rules Engine**.
  - If you are using Wolters Kluwer, click **Regulatory Compliance > WK Regulatory Events** and then click **Wolters Kluwer Rules Engine**.
3. Select the rules that you want to enable or disable by clicking its check box in the first column.
4. Click **Copy**.
5. Type a **Name** for the rule.
6. Edit the rule definition.  
For more information, see [“Conditions in rules” on page 912](#) and [“Target actions in rules” on page 913](#).
7. Click **Done**.

## Enabling and disabling rules

Enable a rule to make it active.

### About this task

When a rule is enabled, it is used to process incoming Regulatory Events. When you create a new rule, it is enabled by default.

When a rule is disabled, it is not used but it is still available in the **Rules Engine**.

To do this task, you need the **SOX > Administration > Rules Engine** permission.

### Procedure

1. Click  to open the Primary menu.
2. Do one of the following steps:
  - If you are using Thomson Reuters Regulatory Intelligence, click **Regulatory Compliance > TRRI Regulatory Events** and then click **TRRI Rules Engine**.
  - If you are using Wolters Kluwer, click **Regulatory Compliance > WK Regulatory Events** and then click **Wolters Kluwer Rules Engine**.
3. Select the rules that you want to enable or disable by clicking the check boxes in the first column.  
The **Enabled** column displays a check mark for rules that are enabled and an **X** for rules that are disabled.
4. Click **Enable** or **Disable**.
5. Clear all check boxes to hide the toolbar.

## Editing rules

You can edit rules to change their conditions, target actions, users and groups, and criticality. You cannot change the name of a rule.

### About this task

To do this task, you need the **SOX > Administration > Rules Engine** permission.

### Procedure

1. Click  to open the Primary menu.
2. Do one of the following steps:
  - If you are using Thomson Reuters Regulatory Intelligence, click **Regulatory Compliance > TRRI Regulatory Events** and then click **TRRI Rules Engine**.
  - If you are using Wolters Kluwer, click **Regulatory Compliance > WK Regulatory Events** and then click **Wolters Kluwer Rules Engine**.
3. Click the name of the rule that you want to edit.  
**Tip:** To sort the rules, click a column heading.
4. Make your changes.  
You cannot change the **Name** of the rule.
5. Click **Done**.

## RCM Theme Deployer

---

The RCM Theme Deployer is a tool that you can use to automatically create requirements that are ready for assessment. The tool can also automatically create the appropriate associations.

The RCM Theme Deployer helps you to create the theme structure for business entities. Once you select a theme to deploy to the business entities, the structure is created, including the compliance plan, compliance theme, and the relevant requirement evaluation records beneath the theme, linked to the relevant Control objects.

Users can launch the Theme Deployer in two ways: from the Compliance Theme object (pushing a theme out to business entities) or from the Compliance Plan object (pulling themes into a specific business entity).

The Theme Deployer creates the Compliance Theme object and its related child requirements, represented as Requirement Evaluation (ReqEval) objects. The ReqEval objects are used to evaluate the requirements in an assessment. An association is created between the library Requirement object and the ReqEval object.

You can also link the ReqEval and relevant control instances in that area of the business.

You can also copy library instances of the related customer controls that do not already exist in the target business area.

**Note:** When users run the RCM Theme Deployer, they will be copying and/or linking objects from the configured Library folders to the configured business entity objects. The users must have the following security access:

- Read access to the Library folders they are copying from
- Read, Write, and Associate access to the business entity objects that they are writing to

## Process overview for the RCM Theme Deployer

You can set up the IBM OpenPages Regulatory Compliance Management Theme Deployer if you have the 7.3 or later solutions schema.

If you upgraded or migrated to 9.0, do the following steps to complete the setup:

- [“Setting up auto-naming for RCM objects” on page 916](#)
- [“Updating views for the RCM Theme Deployer” on page 916](#)
- [“Using the RCM configuration tool” on page 917](#)

If you did a fresh installation, do the following tasks::

- [“Updating views for the RCM Theme Deployer” on page 916](#)
- [“Using the RCM configuration tool” on page 917](#)

## Setting up auto-naming for RCM objects

If you upgraded or migrated to 9.0, you must set up auto-naming for the **CompliancePlan** object. Optionally, you can also set up auto-naming for the **ComplianceTheme** and **ReqEval** objects.

### Procedure

1. Log in to OpenPages as a user with administrative privileges.
2. Click  > **System Configuration** > **Settings**.
3. Set up auto-naming for the **CompliancePlan** object.
  - a) Expand the **Applications** > **GRCM** > **Auto Naming** > **CompliancePlan** > **Auto-Named** folder.
  - b) Set the value of **Copied Object** to True.
  - c) Set the value of **New Object** to True.
4. Set up auto-naming for the **ComplianceTheme** object.
  - a) Expand the **Applications** > **GRCM** > **Auto Naming** > **ComplianceTheme** > **Auto-Named** folder.
  - b) Set the value of **Copied Object** to True.
  - c) Set the value of **New Object** to True.
5. Set up auto-naming for the **ReqEval** object.
  - a) Expand the **Applications** > **GRCM** > **Auto Naming** > **ReqEval** > **Auto-Named** folder.
  - b) Set the value of **Copied Object** to True.
  - c) Set the value of **New Object** to True.

## Updating views for the RCM Theme Deployer

Update views to use the RCM Theme Deployer.

In the views for the following object types, ensure the **Compliance Theme** field, when present, is set to **Read Only**:

- **Compliance Theme**
- **Compliance Plan**

In the views for the following object types, ensure that the **Library ID** field set to **Read Only**:

- **Compliance Theme**
- **Compliance Plan**
- **Requirement**
- **ReqEval**

For information about working with views, see [Chapter 14, “Views,” on page 247](#).

# Using the RCM configuration tool

You can use the RCM configuration tool to configure IBM OpenPages Regulatory Compliance Management (RCM).

## About this task

When you type fields, use the format *<Field Group>:<Field Name>*, ensure that no spaces exist before and after the colon. For example, type RCM-Req:Reqt\_Owner. For system fields, you can type just the field name.

To add another field, click the plus sign, and then type the field.

**Note:** Rich text fields are shown in plain text in the RCM Theme Deployer.

## Procedure

1. Log in to OpenPages as an administrator.
2. Open the RCM configuration tool in a new browser tab or window.

The URL is:

`http://<hostname>:<port>/app/solutions/rmc/config/showConfig#/editconfig`

3. Log in with your OpenPages user account. You must be a member of the OPAdministrators group to access the tool. You can have the tool open and simultaneously be logged in to OpenPages to work on other administration tasks.

4. Expand the **Common Properties** section.
5. Enter the following information.

RCM uses these paths to locate the libraries. Use a forward slash (/) as a separator. For example, enter /Library/Control.

- a) Enter the path for the **Control Library Folder**.
- b) Enter the path for the **Requirement Library Folder**.
- c) Enter the path for the **Theme Library Folder**.
- d) Enter the path for the **Root Entity Folder**.

The **Root Entity Folder** is used to locate the business unit hierarchy.

6. Expand the **Theme Deployer Properties** section.

7. Under **Control Deployment Options**, select one or more of **Create & Link**, **Link**, and **None**.

These options define the deployment of controls during the deployment of themes. The selections that you make are displayed as options to the end user within the **Theme Deployer** helper.

- Select **Create & Link** to give the end user the option to create controls, if they do not exist, and to associate existing controls to the deployed Requirement Evaluation (ReqEval) objects.
- Select **Link** to give the end user the option to associate existing controls to the deployed Requirement Evaluation objects. New objects are not created.
- Select **None** to give the end user the option of not deploying any controls during the theme deployment process.

8. In the section **Theme Fields to be Copied**, specify the fields to be copied from the Theme Library to the deployed Compliance Theme.

By default, the field to be copied is set to **Name**, unless auto-naming is enabled. For information about auto-naming, see [“Setting up auto-naming for RCM objects” on page 916](#).

9. In the section **Requirement Fields to be Copied**, specify the fields to be copied from the library Requirement object to the Requirement Evaluation object that is created during deployment.

By default, the field to be copied is set to **Name**, unless auto-naming is enabled.

During the copy process, a new Requirement Evaluation (ReqEval) object is created. This object might use different field groups and fields than its parent Requirement.

If the source and target fields are different, type the fields separated by the vertical line character (|). For example, type RCM-Req:Overall Requirement Score|RCM-Req-Eval:Applied Overall Rating.

10. If you selected the **Create & Link** option, use the **Control Fields to be Copied** to enter the fields to be copied from the library Control object to the Control object that is created during the deployment process.

By default, the field to be copied is set to **Name**, unless auto-naming is enabled.

This field applies only if you selected **Create & Link** as a control option, because this option creates a Control during the deployment process.

11. In the section **Define BE Grid Columns**, enter the Business Entity grid columns to be displayed in the helper when accessed through the Compliance Theme.
12. In the section **Define Theme Grid Columns**, enter the Theme grid columns to be displayed in the helper when accessed through the Compliance Plan.

13. Click **Validate** to validate your entries.

The folder paths are validated to ensure that they are in the correct format, and that the folders exist.

The fields are validated to ensure that the fields that you selected in **Define BE Grid Columns** and **Define Theme Grid Columns** exist in the application.

14. Click **Save**.

# Chapter 38. Configuring IBM OpenPages Third Party Risk Management

You can configure IBM OpenPages Third Party Risk Management (TPRM).

For example, you can import data from SecurityScorecard and Supply Wisdom.

## SecurityScorecard connector for IBM OpenPages Third Party Risk Management

IBM OpenPages Third Party Risk Management (TPRM) includes a connector for SecurityScorecard.

The SecurityScorecard connector enables you to import security ratings from SecurityScorecard into Vendor objects in OpenPages. You can then view the ratings in OpenPages.

**Note:** To use the connector, you must meet the following prerequisites:

- You must have a SecurityScorecard subscription. Work with SecurityScorecard to set up access. For more information, contact SecurityScorecard.
- You must install the SecurityScorecard connector. For more information, contact IBM OpenPages Support.
- In SecurityScorecard, add vendors to your portfolio. You can use your default portfolio or create a new portfolio.

When OpenPages imports ratings from SecurityScorecard, it does the following tasks:

- Looks for vendors in OpenPages that match the companies in your SecurityScorecard portfolio, based on the Vendor URL field.
- If the vendor exists in OpenPages, updates the fields in the Vendor object with the ratings from SecurityScorecard.
- If the vendor does not exist in OpenPages, creates a new Vendor object with the data from SecurityScorecard.

### Configuring the SecurityScorecard connector

Configure the import of SecurityScorecard data into IBM OpenPages with Watson.

#### Before you begin

To connect to SecurityScorecard, you need all of the following items:

- Your SecurityScorecard API token.
- The name of the portfolio in SecurityScorecard that contains the data that you want to import.

#### About this task

To do this task, you need the following application permissions:

- **SOX > Administration > Security Scorecard Feed**
- **SOX > Administration > Scheduler**

#### Procedure

1. Log in.
2. Click  > **Solution Configuration > Scheduler**.

3. Click the **Security Scorecard** job.
4. Click **Edit**.
5. Configure the connector:
  - Click **Portfolio** and type the name of your SecurityScorecard portfolio. The default is called **My Portfolio**.
  - Click **Token** and type your SecurityScorecard API token.
  - Verify the value in the **Host** field.
  - In the **Schedule** section, click **Edit**. Set the schedule for the import from SecurityScorecard.
6. Click **Done**.  
The connector is configured and the import is scheduled.
7. If you want to import data from SecurityScorecard now, click the checkbox next to the **Security Scorecard** job and then click **Start Job** ▶.

## What to do next

To see the progress of an import, go to  > **Solution Configuration** > **Scheduler**, click the **Security Scorecard** job, and then click the **Executions** tab. Click a process to view the log.

## Supply Wisdom connector

---

IBM OpenPages Third Party Risk Management (TPRM) includes a connector for Supply Wisdom. You can also use the connector with IBM OpenPages Business Continuity Management.

You can use the Supply Wisdom connector to import vendor details, ratings, and alerts from Supply Wisdom into OpenPages. You can then view the data in OpenPages.

**Note:** To use the connector, you must meet the following prerequisites:

- You must have a Supply Wisdom subscription. Work with Supply Wisdom to set up access. For more information, contact Supply Wisdom.
- You must install the Supply Wisdom connector. For more information, contact IBM OpenPages Support.

By default, the connector imports vendors, locations, and alerts, but you can change these defaults when you configure the import.

When OpenPages imports data from Supply Wisdom, the import process does the following tasks:

- Looks for vendors in OpenPages that match the vendors in your Supply Wisdom subscription.
- If the vendor exists in OpenPages, the import process creates a Supply Wisdom object as a child of the Vendor object. The risk ratings are stored in the Supply Wisdom object. The Supply Wisdom objects are created under /BusinessEntity/Library/SupplyWisdom.
- Imports any Event Monitoring alerts for the vendors and stores them in a Supply Wisdom Parent Alert object.
- Imports the data about the locations in which the Vendor operates and stores it in a Location object.
- If a Supply Wisdom object already exists for the Vendor, the import process updates the fields in the Supply Wisdom object with the risk scores from Supply Wisdom. The Supply Wisdom object stores the current scores and the scores from the previous four quarters.
- If the vendor does not exist in OpenPages, the import process creates a Vendor object and a Supply Wisdom object with the data from Supply Wisdom.

# Configuring the Supply Wisdom connector

Configure the import of Supply Wisdom data into IBM OpenPages with Watson.

## Before you begin

To connect to Supply Wisdom, you need all of the following items:

- The Supply Wisdom URL.
- Your Supply Wisdom username and password.

## About this task

To do this task, you need the following application permissions:

- **SOX > Administration > SupplyWisdom Feed**
- **SOX > Administration > Scheduler**

## Procedure

1. Log in to OpenPages.
2. Click  > **Solution Configuration > Scheduler**.
3. Click the **SupplyWisdom** job.
4. Click **Edit**.
5. Configure the connector:
  - Verify the value in the **Host** field.
  - Click **Password** and type your Supply Wisdom username.
  - Click **Username** and type your Supply Wisdom username.
  - If you want to import alerts, set **Import Alerts** to true and set **Max Days of Alerts to Get**.
  - If you want to import location data, set **Import Location** to true.
  - If you want to import vendor details, set **Import Vendors** to true.
  - In the **Schedule** section, click **Edit**. Set the schedule for the import from Supply Wisdom.
6. Click **Done**.  
The connector is configured and the import is scheduled.
7. If you want to import data from Supply Wisdom now, click the checkbox next to the **SupplyWisdom** job and then click **Start Job** .

## What to do next

To see the progress of an import, go to  > **Solution Configuration > Scheduler**, click the **SupplyWisdom** job, and then click the **Executions** tab. Click a process to view the log.

## RapidRatings connector for IBM OpenPages Third Party Risk Management

---

IBM OpenPages Third Party Risk Management (TPRM) includes a connector for RapidRatings.

You can use the RapidRatings connector to import vendor details and financial ratings from RapidRatings into OpenPages. You can then view the vendors and ratings in OpenPages.

**Note:** To use the connector, you must meet the following prerequisites:

- You must have a RapidRatings subscription. Work with RapidRatings to set up access. For more information, contact RapidRatings.

- You must install the RapidRatings connector. For more information, contact IBM OpenPages Support.

When OpenPages imports data from RapidRatings, the import process does the following tasks:

- Looks for vendors in OpenPages that match the vendors in your RapidRatings subscription.
- If the vendor exists in OpenPages, the import process creates a RapidRatings object as a child of the Vendor object. The risk ratings are stored in the RapidRatings object. The RapidRatings objects are created under /BusinessEntity/Library/VRM/VRMLibrary/RapidRatings.
- If a RapidRatings object already exists for the Vendor, the import process updates the fields in the RapidRatings object with the risk ratings from RapidRatings. The RapidRatings object stores the current ratings and the ratings from the previous four quarters.
- If the vendor does not exist in OpenPages, the import process creates a Vendor object and a child RapidRatings object with the data from RapidRatings.

## RiskRecon connector for IBM OpenPages Third Party Risk Management

---

IBM OpenPages Third Party Risk Management (TPRM) includes a connector for RiskRecon.

You can use the RiskRecon connector to import cybersecurity ratings and scores for vendors from RiskRecon into OpenPages. You can then view the ratings in OpenPages.

**Note:** To use the connector, you must meet the following prerequisites:

- You must have a RiskRecon subscription. Work with RiskRecon to set up access. For more information, contact RiskRecon.
- You must install the RiskRecon connector. For more information, contact IBM OpenPages Support.

When OpenPages imports data from RiskRecon, the import process does the following tasks:

- Looks for vendors in OpenPages that match the vendors in your RiskRecon portfolio.
- If a vendor in your RiskRecon portfolio does not exist in OpenPages, the job creates a Vendor object.
- The import process updates the OPSS-RiskRecon-Vendor field group on the Vendor object and creates RiskRecon Ratings objects as children of the Vendor object. The RiskRecon Ratings objects are created under /BusinessEntity/Library/VRM/VRMLibrary/RiskRecon. The OPSS-RiskRecon-Vendor field group stores the risk ratings and scores at the company level while the RiskRecon Ratings objects store the ratings and scores at the category and subcategory levels.
- If RiskRecon data exists for the Vendor, the import process updates the OPSS-RiskRecon-Vendor field group and the RiskRecon Ratings objects with the most recent ratings and scores from RiskRecon.

If you remove a vendor from your RiskRecon portfolio, any existing RiskRecon data in OpenPages is not deleted. If you delete a vendor in OpenPages, the vendor is added again when you run the job, unless you also remove the vendor from your RiskRecon portfolio.

## Configuring the RiskRecon connector

Configure the import of RiskRecon data into IBM OpenPages with Watson.

### Before you begin

To connect to RiskRecon, you need all of the following items:

- The RiskRecon API URL.
- Your RiskRecon API key.

### About this task

To do this task, you need the following application permissions:

- **SOX > Administration > RiskRecon Feed**
- **SOX > Administration > Scheduler**

## Procedure

1. Log in to OpenPages.
2. Click  > **Solution Configuration > Scheduler**.
3. Click the **RiskRecon** job.
4. Click **Edit**.
5. Configure the connector:
  - Click **API Key** and type your RiskRecon API key.
  - Verify the value in the **API Host** field. This field stores the URL for the RiskRecon API.
  - In the **Schedule** section, click **Edit**. Set the schedule for the import from RiskRecon.
6. Click **Done**.  
The connector is configured and the import is scheduled.
7. If you want to import data from RiskRecon now, click the checkbox next to the **RiskRecon** job and then click **Start Job** .

## What to do next

To see the progress of an import, go to  > **Solution Configuration > Scheduler**, click the **RiskRecon** job, and then click the **Executions** tab. Click a process to view the log.



# Appendix A. The Notification Manager

---

The Notification Manager is a JSP-based report and notification add-on utility for IBM OpenPages with Watson. It automatically creates notification emails when specified criteria are met.

**Note:**

- If you are using IBM OpenPages for IBM Cloud Pak for Data, use a JSP report job in the Scheduler instead. The Notification Manager is not available in IBM OpenPages for IBM Cloud Pak for Data. For more information, see [“Defining a job that runs a JSP report” on page 438](#).
- If you are using IBM OpenPages with Watson, consider using a JSP report job in the Scheduler instead of the Notification Manager. For more information, see [“Defining a job that runs a JSP report” on page 438](#).

With the Notification Manager, administrators can define a set of object properties and values that trigger the sending of a notification email to a user. The user responsible for the item will receive the email, alerting the user to their necessary tasks.

For example, a notification event can be set to run nightly that will send a notification email to all users who have Tests that do not have completed Test Results associated with them.

To use the Notification Manager tool, you need the **SOX > Administration > Notification Manager** application permission.

## Why would I use Notifications?

Notifications allow you to alert people that important dates are approaching, and remind them that they still have outstanding tasks to perform before the date arrives.

Since notification can be tied to the value of an object property, you can target the reminder to only those people who meet the criteria for the notification.

For example, you can set up a notification to remind all Control owners who have controls that have a value of "Undetermined" for the Control Evaluation field, and set the notification to start 20 days after the beginning of the quarter.

## Notification reports

Decide where you want to store the report pages and page templates for notifications. For example, you might use the Reporting/[locale]/SOX/Notifications folder.

Decide where you want to store the report pages and page templates for notifications. For example, you might use the Reporting/[locale]/SOX/Notifications folder.

When a notification report is run, a notification email is generated for the Executive or Primary Owners detailing the objects that require attention.

## Requirements for setting up a notification

---

In order to set up a notification event, you must have the following:

- A user account with the application permissions for publishing pages and templates. For more information, see [“Application permissions not contained under the SOX heading” on page 58](#))
- Administrator access to the IBM OpenPages with Watson server machine (for scheduling reports to run automatically)

**Tip:** You can also run Notification Manager from a remote system, such as your laptop. For more information, see [“Installing tools and utilities \(IBM OpenPages with Watson\)” on page 692](#)

- Your notification mail server configured. For more information, see [“Configuring your mail server” on page 486](#).

# Setting up a notification

---

Three procedures are required to set up and execute a notification.

- “Task 1: Creating a page template” on page 926
- “Task 2: Creating the notification” on page 926
- “Task 3: Triggering the notification” on page 927

After each task is completed, you can run the notification manually or schedule it to run automatically.

## Task 1: Creating a page template

The first step in setting up a notification is to create a page template that the notification report is based on.

### Before you begin

Ensure that your objects have the necessary information that will be required by the notification report. If the objects are not up-to-date, the report will not find the data it needs and will either return a sub-set of the entire results, or fail to run at all.

### Procedure

1. Log on to OpenPages with Watson as a user with **Publishing** privileges set.
2. Click  > **System Configuration** > **Pages and Templates**.
3. Navigate to the Reporting/[locale]/SOX/Notifications folder and select it with a check mark.
4. Click **Add Page Template**. The **New Page Template** screen is displayed.
5. Do the following:
  - a) Enter a name for the page template.
  - b) Select an **Output file extension**.
  - c) Select a **Template JSP**.
  - d) Enter a description for the page template.
  - e) Click **Save**.

## Task 2: Creating the notification

The second task in setting up a notification is to create the notification.

### Procedure

1. Log on to the OpenPages with Watson as a user with **Publishing** privileges set.
2. Click  > **System Configuration** > **Pages and Templates**.
3. Navigate to the Reporting/[locale]/SOX/Notifications folder and select it with a check mark.
4. Click **New Page**. The **New Page** screen is displayed.
5. Do the following:
  - a) Enter a name and description for the notification report.
  - b) Choose the page template that you already created in Task 1.
  - c) Enter the information for your notification type in **Page Details**.
  - d) Click **Save**.

## Task 3: Triggering the notification

You can run notification reports from a **Reporting > Notifications** panel on the Dashboard, or you can use the provided command-line interface to run the notification reports from outside the IBM OpenPages with Watson environment.

**Tip:** You can also run Notification Manager from a remote system, such as your laptop. For more information, see “[Installing tools and utilities \(IBM OpenPages with Watson\)](#)” on page 692

If you are using IBM OpenPages for IBM Cloud Pak for Data, use a JSP report job in the Scheduler instead. The reporting interface and the Notification Manager utility are not available in IBM OpenPages for IBM Cloud Pak for Data. For more information, see “[Defining a job that runs a JSP report](#)” on page 438.

### Using the UI

Running a notification report works the same as running any other report through the user interface.

#### Before you begin

If it does not display, add a Reports panel to the Dashboard. Choose Reports in **Panel Type**, All Reports in **Data Source**, and save the panel.

#### Procedure

1. Log on.
2. From the Dashboard, click the **Reporting** panel (it might be named differently on your system).
3. Expand the **Notifications** folder to display the notification reports.
4. Choose the notification report you want to run and click the name of the report.

The results of the report are displayed.

### Using the Notification Manager command-line interface

You can manually run the Notification Manager from a command or shell window, or you can use standard operating system scheduler functions to automatically run the Notification Manager command file at a specified time.

For example, in Windows, you could use the built-in Windows scheduler. In Linux, you could set up a cron job.

You can run a single report, an entire folder of reports, and run a single report against multiple data sets by providing parameters to the report directly through the command line.

The Notification Manager command file is named as follows:

#### Windows

NotificationManager.cmd

#### Linux

NotificationManager.sh

The file is located in the `<OP_Home>/bin` directory of your IBM OpenPages with Watson installation.

### The Notification Manager command-line interface syntax

This topic contains the Notification Manager command-line interface syntax and parameters.

#### Syntax

```
NotificationManager -Username <user_name> -Password <password>
-NotificationProgram <full_path_to_notification_report>|-ProgramFolder
<path_to_folder-containing-notification-reports> [-SaveOutput <true|false>]
```

```

[-LogSession <true|false>]
[-<parameter_name> <parameter_value>] [-ParameterFile <full_path_to_file>]

```

## Parameters

All parameters are in the syntax `-parameter "value or string"`. If the value of any parameter contains spaces, that value must be contained within quotation marks.

Table 255. Notification Manager parameters	
Parameter	Description
<code>-Username</code>	The name of a valid IBM OpenPages with Watson user with permission to run the notification reports.
<code>-Password</code>	The password for the user name set in <code>-Username</code> .
<code>-NotificationProgram</code>	(Required unless <code>-ProgramFolder</code> is specified) The full path to the notification report the command will run, starting with the Reporting folder. Should not begin with a leading slash.  Example  <code>-NotificationProgram "Reporting\SOX\Notifications\Test Notifications Report"</code>
<code>-ProgramFolder</code>	(Required unless <code>-NotificationProgram</code> is specified) Specifies a folder containing notification reports. All reports in that folder will be executed when the command is run.  Example  <code>-ProgramFolder "Reporting\SOX\Notifications"</code>
<code>-SaveOutput</code>	(Optional) Can be <b>true</b> or <b>false</b> . If set to true, the output of the report will be saved to an output file in the <code>output_files</code> directory under the <code> bin NotificationManager</code> directory. If the parameter is not present, no output file will be created.  The file name is the name of the notification report (or folder) with an "html" extension. If an output file with that name already exists, a timestamp extension will be added to the end of the existing file's name and the older file will be moved to the <code>output_files archive</code> folder.  Example  <code>Undetermined Controls.html.200406060103</code>
<code>-LogSession</code>	(Optional) Can be set to <b>true</b> . If set, the activities of the <code>NotificationManager</code> will be written to a log file. The log file will be located in the <code>logs</code> directory under the <code> aurora bin NotificationManager</code> directory.  The name of the log file is <code>NotificationManager.log</code> . The file has a maximum size of 1 MB, and will be rotated into the <code> logs archives</code> directory when the limit is exceeded.

Table 255. Notification Manager parameters (continued)

Parameter	Description
<p>-&lt;parameter_name&gt; &lt;parameter_value&gt;</p> <p>Where:</p> <p>&lt;parameter_name&gt; is the name of a specific parameter</p> <p>&lt;parameter_value&gt; is the value of that parameter</p>	<p>(Optional) If you want to pass a value for a specific notification report parameter, you can include the parameter and value directly in the command line. The parameter name must match the report parameter name exactly.</p> <p>You can see the parameter names in OpenPages with Watson. Click  &gt; <b>System Configuration &gt; Pages and Templates</b>, navigate to the folder that contains the report page, and then click the page. The parameter names are shown in the <b>Parameters</b> section.</p> <p>Examples</p> <ul style="list-style-type: none"> <li>• -mailServer mail.openpages.com</li> <li>• -generalMessage "Please do not ignore this email."</li> </ul>
<p>-ParameterFile</p>	<p>Specifies a text file containing a list of parameter value pairs (equivalent to entering individual -parameter "value or string" entries into the command line directly). Each parameter value pair should be on a single line.</p> <p>Value is the full path to the file, including the file name.</p> <p>Example - for Windows:</p> <pre>-ParameterFile "c:\OpenPages\bin\NotificationManager\notification_parameters.txt"</pre>



---

# Appendix B. Properties and parameters

IBM OpenPages with Watson includes different properties files. Depending on the configuration task that you perform, you edit one or more of the properties files.

## Aurora properties and parameters

---

Depending on the configuration task that you perform in IBM OpenPages with Watson, you might need to edit the parameters in the `aurora.properties` file.

The `<OP_HOME>/aurora/conf/aurora.properties` file parameters are described in the following list.

**Note:** If you change the parameter values, you must restart the application servers.

### Application server properties

#### **aurora.appserver**

The type of Java Platform Enterprise Edition (J2EE) application that is used.

Possible value: `websphere`.

This setting is deprecated.

#### **aurora.initialcontext.factory**

Java Naming and Directory Interface (JNDI) initial context factory.

This setting is deprecated.

### Database properties

#### **database.type**

Type of database (Oracle or DB2).

#### **database.URL**

Java Database Connectivity (JDBC) URL.

#### **database.DRIVER**

Java Database Connectivity (JDBC) driver.

#### **database.USERID**

Database user name.

#### **database.PASSWORD**

Database password (encrypted).

### IBM Db2 database properties

#### **database.NAME**

Database name.

#### **database.HOSTNAME**

Database hostname.

#### **database.PORT**

Database port.

#### **database.CATALOG\_NAME**

Database catalog name.

## **Database pool properties**

### **database.pool.testonreserve**

Flag to test a connection before returning it from the pool.

Possible values: true or false.

### **database.test.connection.sql**

Specify a Microsoft SQL database with which to test the connection.

The default value is: *select sysdate from dual*.

## **Java Transaction API (JTA) properties**

### **jta.initialcontext.factory**

Java Naming and Directory Interface (JNDI) Initial Context Factory.

This setting is deprecated.

### **jta.jndi.transaction**

Java Naming and Directory Interface (JNDI) name for User Transactions.

This setting is deprecated.

## **Full text search properties**

**Note:** These legacy settings are no longer used.

### **fulltext.index.directory**

Full text index folder.

### **fulltext.index.exclude**

File extensions to be excluded.

The default values are: xra xrl pagespec pagetemplate xrt cha xsd.

## **Java Message Service (JMS) properties**

### **jms.initialcontext.factory**

Java Naming and Directory Interface (JNDI) Initial Context Factory.

This setting is deprecated.

### **jms.topic.RepositoryTopic**

Java Message Service (JMS) topic name.

### **jms.topic.ResourceCacheTopic**

Java Message Service (JMS) topic name.

## **Security service properties**

### **security.accesstoken.timeout**

Session token timeout, in minutes.

The default value is 3000000.

### **security.system.password**

Password of the system OPSSystem user.

## **AppServer specific properties**

### **appserver.install.directory**

The installation folder of the OpenPages application (OP\_HOME).

## **Third-party reporting-specific properties**

### **cognos.report.output.dir**

Temporary folder for reports.

## **Application URL property**

### **application.url.path**

Base URL of the application.

**Note:** In a load balanced environment, the `application.url.path` value is the fully qualified domain name of the load balancer and its port number.

## **Application server WorkManager properties**

### **workmanager.jndi.name**

Java Naming and Directory Interface (JNDI) name of the application server work manager.

This setting is deprecated.

### **workmanager.impl.classname**

Work manager implementation class.

This setting is deprecated.

## **Enterprise JavaBeans (EJB) properties**

### **server.use.local.ejb**

Must be `true`.

This setting is deprecated.

## **Other properties**

### **enforce.browser.support**

Enables or disables the **Allowed Browsers** feature. For more information, see [“Specify the browsers that can access IBM OpenPages” on page 479](#).

Value: `true` or `false`

## **OpenPages server properties and parameters**

---

Depending on the configuration task that you perform in IBM OpenPages with Watson, you might need to edit the parameters in the `Server<#>-server.properties` file.

The OpenPages server properties are described in the following list.

**Note:** If you change the property values, you must restart the application servers.

## **Cache properties**

### **cache.synchronizer.classname**

Non-configurable system parameter.

### **cache.listener.enabled**

Non-configurable system parameter.

### **cache.notifier.enabled**

Non-configurable system parameter.

### **jms.topic.CacheTopic**

Non-configurable system parameter.

## Web client properties

### **webclient.http.server.protocol**

Enter the value `http` or `https`, based on your configuration. The default value is `http`.

### **webclient.http.server.name**

Non-configurable system parameter.

### **webclient.http.server.port**

If you change the OpenPages application port number (default for non-SSL: 10108), update the application port value in this parameter.

## Other

### **async.calculation.enabled**

Enables or disables asynchronous processing of calculations.

If you are using clustered application servers, setting this property to `true` can help performance by managing the processing workload for calculations. You can enable or disable this property on a server-by-server basis to control the workload.

Value: `true` or `false`

## Sosa properties and parameters

---

Depending on the configuration task that you perform in IBM OpenPages with Watson, you might need to edit the parameters in the `Server<#>-sosa.properties` file.

The `Server<#>-sosa.properties` file parameters are described in the following list.

**Note:** If you change the parameter values, you must restart the application servers.

### Application URL properties

#### **application.url.path**

Configurable application URL.

`http\://<hostname>\:<port>/openpages`

Where:

- `hostname` is fully qualified, and includes the local host and the parent domain name.
- `<port>` is the OpenPages application port number (for example, 10111).

**Note:** In a load balanced environment, the `application.url.path` value is the fully qualified domain name of the load balancer and its port number.

#### **application.context**

Configurable application context.

`/openpages`

### Service URL properties

#### **openpages.service.initial.ctx.factory**

Non-configurable system parameter.

## Tools properties and parameters

---

Depending on the configuration tasks that you perform in IBM OpenPages with Watson, you might need to edit the properties in the `openpages-tools-client.properties` file.

The `openpages-tools-client.properties` file is used by OpenPages tools such as ObjectManager, Notification Manager, and command-line utilities.

The file is located on each application server in the `<OP_HOME>/bin` directory.

**rest.url.path**

The base URL of the public REST API on the application server.

**IBM OpenPages with Watson**

```
https\://<host>\:<port>/grc/api
```

Replace *<host>* with `localhost` or with the hostname of the OpenPages application server. You can use `localhost` if the tools and utilities will be run on the application server.

Replace *<port>* with the OpenPages application server's port number.

For example:

```
https\://localhost\:10111/grc/api
```

**IBM OpenPages for IBM Cloud Pak for Data**

See [Installing tools and utilities in Cloud Pak for Data](#).

**insecure.skip.tls.verify**

If set to `true`, the application server's TLS (SSL) certificate is not checked for validity when you run tools such as ObjectManager.

If set to `false` or if the `insecure.skip.tls.verify` is not specified in the `openpages-tools-client.properties`, the application server's certificate is checked for validity. The TLS check occurs when a tool (such as ObjectManager) communicates with the REST API on the application server. The check passes if either of the following conditions is true:

- The server's certificate is valid (it is not self-signed).
- The server's certificate is self-signed but exists in the client's truststore.

Allowed values: `true` or `false`

Default value: `false`

If the URL in `rest.url.path` uses HTTP, the `insecure.skip.tls.verify` property is ignored.

**max.req.body.size.mb**

The maximum request size (in MB) of requests that are sent from client tools, such as ObjectManager, to the server's REST API. A request that is larger than this threshold is automatically divided into chunks, which are then sent separately.

For example, suppose that your web server sets an upload limit of 50 MB. This upload limit means that any requests from client tools must be smaller than 50 MB. To meet this requirement, you can set `max.req.body.size.mb=50`. Now, suppose that you use ObjectManager to load 100 MB of data. Your upload is automatically broken down into two 50 MB chunks so that the upload does not exceed the 50 MB threshold.



---

# Appendix C. Troubleshooting and support for IBM OpenPages with Watson

To isolate and resolve problems with IBM products, use the troubleshooting and support information. This information contains instructions for using the problem-determination resources that are provided with IBM products, including OpenPages with Watson.

## Techniques for troubleshooting problems

---

*Troubleshooting* is a systematic approach to solving a problem. The goal of troubleshooting is to determine why something does not work as expected and how to resolve the problem. Certain common techniques can help with the task of troubleshooting.

The first step in the troubleshooting process is to describe the problem completely. Problem descriptions help you and IBM OpenPages Support know where to start to find the cause of the problem. This step includes asking yourself basic questions:

- What are the symptoms of the problem?
- Where does the problem occur?
- When does the problem occur?
- Under which conditions does the problem occur?
- Can you reproduce the problem?

The answers to these questions typically lead to a good description of the problem, which can then lead you to a problem resolution. For more information, see [“Searching knowledge bases” on page 938](#).

### What are the symptoms of the problem?

When you begin to describe a problem, the most obvious question is “What is the problem?” This question might seem straightforward; however, you can break it down into several more-focused questions that create a more descriptive picture of the problem. These questions can include:

- Who, or what, is reporting the problem?
- What are the error codes and messages? Did you turn on enhanced error messaging to get more details about the error?

For more information about enhanced error messaging, see [“Enable users to get error message details for troubleshooting” on page 514](#).

- How does the system fail? For example, is it a loop, hang, crash, performance degradation, or incorrect result?

### Where does the problem occur?

Determining where the problem originates is not always easy, but it is one of the most important steps in resolving a problem. Many layers of technology can exist between the reporting and failing components. Networks, disks, and drivers are only a few of the components to consider when you are investigating problems.

The following questions help you to focus on where the problem occurs to isolate the problem layer:

- Is the problem specific to one platform or operating system, or is it common across multiple platforms or operating systems?
- Is the current environment and configuration supported?
- Do all users have the problem?
- (For multisite installations.) Do all sites have the problem?

If one layer reports the problem, the problem does not necessarily originate in that layer. Part of identifying where a problem originates is understanding the environment in which it exists. Take some time to completely describe the problem environment, including the operating system and version, all corresponding software and versions, and hardware information. Confirm that you are running within an environment that is a supported configuration; many problems can be traced back to incompatible levels of software that are not intended to run together or were not fully tested together.

## **When does the problem occur?**

Develop a detailed timeline of events that led up to a failure, especially for those cases that are one-time occurrences. You can most easily develop a timeline by working backward: Start at the time an error was reported (as precisely as possible, even down to the millisecond), and work backward through the available logs and information. Typically, you must look only as far as the first suspicious event that you find in a diagnostic log.

To develop a detailed timeline of events, answer these questions:

- Does the problem happen only at a certain time of day or night?
- How often does the problem happen?
- What sequence of events leads up to the time that the problem is reported?
- Does the problem happen after an environment change, such as upgrading or installing software or hardware?

Responding to these types of questions can give you a frame of reference in which to investigate the problem.

## **Under which conditions does the problem occur?**

Knowing which systems and applications are running at the time that a problem occurs is an important part of troubleshooting. These questions about your environment can help you to identify the root cause of the problem:

- Does the problem always occur when the same task is being performed?
- Does a certain sequence of events need to happen for the problem to occur?
- Do any other applications fail at the same time?

Answering these types of questions can help you explain the environment in which the problem occurs and correlate any dependencies. Even if multiple problems occurred around the same time, the problems are not necessarily related.

## **Can you reproduce the problem?**

From a troubleshooting standpoint, the ideal problem is one that can be reproduced. Typically, when a problem can be reproduced you have a larger set of tools or procedures at your disposal to help you investigate. Problems that you can reproduce are often easier to debug and solve.

However, problems that you can reproduce can have a disadvantage: If the problem is of significant business impact, you do not want it to recur. If possible, re-create the problem in a test or development environment, which typically offers you more flexibility and control during your investigation.

- Can you reproduce the problem on a test system?
- Are multiple users or applications encountering the same type of problem?
- Can you reproduce the problem by running a single command, a set of commands, or a particular application?

## **Searching knowledge bases**

---

You can often find solutions to problems by searching IBM knowledge bases. You can optimize your results by using available resources, support tools, and search methods.

## About this task

You can find useful information by searching the IBM Documentation. However, sometimes you must look beyond the documentation to answer your questions or resolve problems.

## Procedure

To search knowledge bases for information that you need, use one or more of the following approaches:

- Find the content that you need by using the [IBM Support portal](#).

The IBM Support portal is a unified, centralized view of all technical support tools and information for all IBM systems, software, and services. Go to the IBM Support portal to access the IBM electronic support portfolio from one place. You can tailor the pages to focus on the information and resources that you need for problem prevention and faster problem resolution.

- Search for content by using the IBM masthead search.

You can use the IBM masthead search by typing your search string into the **Search** field at the beginning of any ibm.com® page.

- Search for content by using any external search engine, such as Google, Yahoo, or Bing.

If you use an external search engine, your results are more likely to include information that is outside the ibm.com domain. However, sometimes you can find useful problem-solving information about IBM products in newsgroups, forums, and blogs that are not on ibm.com.

**Tip:** Include "IBM" and the name of the product in your search if you are looking for information about an IBM product.

- Join the IBM Governance, Risk and Compliance (GRC) Community. The IBM GRC Community is a communication forum where IBM can share information about OpenPages with the worldwide community of users. Contact IBM Support for instructions to join.

## Getting fixes

---

A product fix might be available to resolve your problem.

## Procedure

To find and install fixes:

1. Determine which fix you need. Go to the [Fix List](#). The Fix List shows a comprehensive list of defect corrections for major releases, fix packs, and interim fixes.
2. At the bottom of the Fix List, click the link to the download document for the fix you want to apply.
3. Download the fix.
4. Apply the fix. Follow the instructions in the "Installation Instructions" section of the download document.
5. Subscribe to receive weekly email notifications about fixes and other IBM Support information. For more information, see ["Subscribing to Support notifications "](#) on page 941.

## Contacting IBM Support

---

IBM Support assists with product defects, answers FAQs, and helps users resolve problems with the product.

### Before you begin

After you tried to find your answer or solution by using other self-help options such as Technotes, you can contact IBM Support.

Before you contact IBM Support, your company or organization must have an active IBM maintenance contract, and you must be authorized to submit problems to IBM. For more information about the types

of available support, see [Support portfolio](#). For more information about how to request access to your company's IBM Support account, see [Requesting access to your company's IBM Support account](#).

## About this task

You can open a case from the web, chat, or by phone. For more information, see [Get help with your products](#).

## Procedure

To contact IBM Support about a problem:

1. Define the problem, gather background information, and determine the severity of the problem.

For more information, see [Open a case](#).

2. Gather the following diagnostic information:

- Environment type (such as production or development).
- Application, release, and patch level (such as IBM OpenPages with Watson 9.0.0.1 or IBM OpenPages for IBM Cloud Pak for Data9.0.2).
- Description of the issue.
- Detailed steps to reproduce the issue.
- Screen captures of the issue.
- Expected and actual results.
- OpenPages with Watson log files. For more information, see *Using log files in the IBM OpenPages with Watson Administrator's Guide*.
- Any workarounds that you implemented.
- The date and time that the issue was encountered.
- Database type and version (such as Oracle 19c or IBM Db2 11.5).

3. Submit the problem to IBM Support in one of the following ways:

- Online through [IBM Support](#). You can open, update, and view all of your cases from the Service Request portlet on the **Service Request** page. This video demonstrates how to open a case from the IBM Support Community: [Open and manage cases](#).
- By phone: For the phone number to call in your region, see the [Directory of worldwide contacts](#) web page.

For more information, see [Get help with your products](#).

## Results

If the problem that you submit is for a software defect or for missing or inaccurate documentation, IBM Support creates an Authorized Program Analysis Report (APAR). The APAR describes the problem in detail. Whenever possible, IBM Support provides a workaround that you can implement until the APAR is resolved and a fix is delivered. IBM publishes resolved APARs on the IBM Support website daily so that other users who experience the same problem can benefit from the same resolution.

[“Contacting IBM Support” on page 939](#)

[“Exchanging information with IBM” on page 940](#)

## Exchanging information with IBM

---

To diagnose or identify a problem, you might be necessary to provide IBM Support with data and information from your system. In other cases, IBM Support might provide you with tools or utilities to use for problem determination.

## Sending information to IBM Support

To reduce the time that is required to resolve your problem, you can send trace and diagnostic information to IBM Support.

### About this task

To submit diagnostic information to IBM Support, add the files to your support case. For more information, see [How to Open a Case](#).

## Receiving information from IBM Support

Occasionally IBM OpenPages Support might ask you to download diagnostic tools or other files. You can use FTP to download these files.

### Before you begin

Ensure that IBM OpenPages Support provided you with the preferred server to use for downloading the files and the exact directory and file names to access.

### Procedure

To download files from IBM Support:

1. Use FTP to connect to the site that IBM OpenPages Support provided and log in as anonymous. Use your email address as the password.
2. Change to the appropriate directory:
  - a) Change to the /fromibm directory.

```
cd fromibm
```

- b) Change to the directory that IBM OpenPages Support provided.

```
cd nameofdirectory
```

3. Enable binary mode for your session.

```
binary
```

4. Use the **get** command to download the file that IBM OpenPages Support specified.

```
get filename.extension
```

5. End your FTP session.

```
quit
```

## Subscribing to Support notifications

To stay informed of important information about the IBM products that you use, you can subscribe to notifications.

### About this task

By subscribing to receive notifications about IBM OpenPages with Watson or IBM OpenPages for IBM Cloud Pak for Data, you can receive important technical information and updates for specific IBM Support tools and resources.

### Procedure

1. Go to the [IBM Support portal](#).

2. Sign in using your IBM ID and password.
3. Click the person icon and select **Settings**.
4. Expand **Case notification settings** and select the options you prefer.

## Missing Administration menu items

---

When you click  to open the **Administration** menu, you might not find all of the menu items you were expecting to see.

To see some menu items, you must have both the required application permissions and access to the associated folders.

For more information about assigning access control to folders, see *Managing system files and folders* in the *System file management* chapter of the *IBM OpenPages with Watson Administrator's Guide*.

For more information about defining application permissions, see *Defining application permissions* in the *Users, groups, and domains* chapter of the *IBM OpenPages with Watson Administrator's Guide*.

### Examples

The menu item  > **Other** > **Logs** is visible only to users who have the All/SOX/Administration/Logs application permission and access to the **LogCollector Documents** folder.

The menu items  > **System Migration** > **Import Configuration** and  > **System Migration** > **Export Configuration** are visible only to users who have access to the **Migration Documents** folder, and who have the All/SOX/Administration/ExportConfiguration application permission for **Export Configuration** and the All/SOX/Administration/ImportConfiguration application permission for **Import Configuration**.

The menu item  > **Integrations** > **Loss Event Entry App** is visible only to users who have Write access to the **End User Applications Config** folder, are members of the OPAdministrators group, and who have access to the following object types: Loss Event, Loss Impact, Loss Recovery, and SOXDocument. See ["Configuring the Loss Event Entry app" on page 839](#).

## Known problems and solutions for global search

---

Issues that are related to the IBM OpenPages with Watson global search component are most commonly encountered when you are setting it up or when it is updated to synchronize the search index for changes that are made to the OpenPages with Watson schema (such as adding or removing object types or fields).

When an administrative operation fails, you can normally resolve these issues by clicking **View Log** to see the log message for the failed global search operation.

The most common failure is that the search service is not started, for which you see this error:

"Could not establish connection to the search engine. Please contact your system administrator."

Ensure that the search service is started or restart to try to resolve the issue.

### Global search start fails

If you configured the global search services to start and stop by using a script and you forgot to stop global search before rebooting the system, when you attempt to start the global search services, the services will fail to start. To fix this issue complete the following steps.

#### Procedure

1. Log on to the search server as a user with administrative privileges.
2. Open a command line on the search server.
3. Go to the <SEARCH\_HOME>/opsearchtools/ directory and run the following commands.

On Microsoft Windows operating systems, run:

```
opsearchtool.cmd clearState -indexname openpages
opsearchtool.cmd clearState -indexname folderacl
```

On Linux operating systems, run:

```
./opsearchtool.sh clearState -indexname openpages
./opsearchtool.sh clearState -indexname folderacl
```

## Global search setup fails

In some rare cases, the global search component might encounter a failure during the creation of the search index, before the operation completes. The failure might be caused by hardware issues, database issues, or a power outage, for example. When this happens, the state of the global search setup is in an undefined state and the **Enable** button might become available, giving the misleading impression that global search was set up successfully. To recover from this state, investigate the root cause, resolve it, and then set up global search again.

### Procedure

1. Investigate and resolve the root cause of the failure.
2. Log on to OpenPages as a user with administrative privileges.
3. Click  > **System Configuration** > **Global Search** and click **Drop**.
4. Wait for the drop process to complete.

If the **Drop** button is not available or if the drop process fails, see “[Forcing a reset of global search](#)” on [page 943](#).

5. Click **Create** to re-create the search index.

## Forcing a reset of global search

In some rare cases, it might be necessary to reset the IBM OpenPages with Watson global search component if you cannot restore it from the **Global Search** administration page. These issues might prevent you from successfully completing tasks in the global search administration page. To resolve these issues, complete the following steps.

### Procedure

1. If you started a global search indexing process from the OpenPages user interface, click **System Configuration** > **Global Search**. Make a note of the **Id** of the indexing process. You need the **Id** in step “9” on [page 944](#).
2. Log on to the search server as a user with administrative privileges.
3. Open a command line on the search server.
4. Go to the `<SEARCH_HOME>/opsearchtools/` directory to run the commands in the following steps.



**Attention:** At the successful completion of each command, the statement "Normal completion of command" should appear. If it does not, contact Customer Support to diagnose the issue.

5. Ensure that Solr is running and is reachable on port 8983. If Solr is not running, then run the following command to start it.

Microsoft Windows:

```
opsearchtool.cmd startSolr
```

Linux:

```
./opsearchtool.sh startSolr
```

6. Run the following commands to stop indexing.

Microsoft Windows:

```
opsearchtool.cmd stopIndexing -indexname openpages
opsearchtool.cmd stopIndexing -indexname folderacl
```

Linux:

```
./opsearchtool.sh stopIndexing -indexname openpages
./opsearchtool.sh stopIndexing -indexname folderacl
```

7. Verify that no opsearchtool.jar processes are running.

On Microsoft Windows operating systems, use the task manager to see whether any opsearchtool.jar processes are running. If there are, terminate them.

On Linux operating systems, use the ps command to see whether any opsearchtool.jar processes are running. If there are, terminate them.

8. Run the following commands to clear any PID states that might still be set if the opsearchtool.jar processes did not end successfully.

Microsoft Windows:

```
opsearchtool.cmd clearState -indexname openpages
opsearchtool.cmd clearState -indexname folderacl
```

Linux:

```
./opsearchtool.sh clearState -indexname openpages
./opsearchtool.sh clearState -indexname folderacl
```

9. If a global search indexing process was started from the OpenPages user interface, run the following commands:

Replace %lrfp-pid% with the **Id** of the indexing process.

Microsoft Windows:

```
opsearchtool.cmd syncIndex -terminatepid %lrfp-pid%
opsearchtool.cmd fullIndex -indexname openpages -terminatepid %lrfp-pid%
opsearchtool.cmd fullIndex -indexname folderacl -terminatepid %lrfp-pid%
```

Linux:

```
./opsearchtool.sh syncIndex -terminatepid %lrfp-pid%
./opsearchtool.sh fullIndex -indexname openpages -terminatepid %lrfp-pid%
./opsearchtool.sh fullIndex -indexname folderacl -terminatepid %lrfp-pid%
```

10. Run the following commands to reset global search.

Microsoft Windows:

```
opsearchtool.cmd resetSolr -indexname openpages
opsearchtool.cmd resetSolr -indexname folderacl
opsearchtool.cmd resetDb
opsearchtool.cmd stopSolr
opsearchtool.cmd startSolr
```

Linux:

```
./opsearchtool.sh resetSolr -indexname openpages
./opsearchtool.sh resetSolr -indexname folderacl
./opsearchtool.sh resetDb
```

```
./opsearchtool.sh stopSolr
./opsearchtool.sh startSolr
```

11. Log on to OpenPages as a user with administrative privileges.
12. Click  > **System Configuration** > **Global Search** and click **Create**.  
**Create** appears only on initial enablement.  
Creating the index also enables global search.

## What to do next

Resetting the global search component does not change your global search settings, such as object types, fields that are enabled for search, registry settings, or property settings.

## Checking for global search setup issues and periodic monitoring

When the incremental indexer is running during global search setup or after setup, some records might not get indexed due to issues with the record, other system errors, or application errors.

### About this task

If the issues are not unrecoverable, they do not impede the setup process or the incremental indexer. However, the records that do not get indexed are logged in an error-log file, with an error message that explains the issue so you can take appropriate action. The error-log files are never rotated. Periodically examine this directory for new error files.

### Procedure

1. Log on to OpenPages as a user with administrative privileges.
2. Go to the directory <SEARCH\_HOME>/opsearchtools/logs\_error/ .
3. Examine this directory for new error files.

## Before you contact IBM OpenPages Support

When you contact IBM OpenPages Support, you need to collect diagnostic data and provide a detailed use case of the issue.

### About this task

Before you contact IBM OpenPages Support to help with resolving global search issues, follow these steps to collect diagnostic data.

**Note:** You do not need to stop global search, the OpenPages application server, the database server, or any other application when you run the **collectDiagData** command.

### Procedure

1. Log in to the OpenPages global search server as a user with administrative privileges.
2. Open a command prompt or a shell window.
3. Go to the <SEARCH\_HOME>/opsearchtools/ folder and run the following commands:
  - Microsoft Windows:

```
mkdir diag
opsearchtool.cmd collectDiagData -diagpath diag
```

- Linux:

```
mkdir diag
./opsearchtool.sh collectDiagData -diagpath diag
```



**Attention:** The **collectDiagData** command might report warning messages that look as if the command failed. This warning can happen due to a number of reasons, such as the data that is being collected cannot be accessed or is not yet available. If you see any such warnings, capture them and include them as part of the diagnostic data to IBM OpenPages Support.

4. Add the contents of the new folder that is created under the diag folder to a compressed file.
5. Send the compressed file and complete details about your issue to IBM OpenPages Support.

## Known problems and solutions for the QRadar integration package

---

Some common problems with QRadar integration package are documented, along with their solutions or workarounds. If you have a problem with QRadar integration package, review the problem-solution topics to determine whether a solution is available to the problem that you are experiencing.

### SDI properties file error message

When you run the assembly line in the qradar\_integration project, you might see one or more warning messages with the error code CTGDIR103W in the IBM Security Directory Integrator (SDI) console.

This message indicates that the enclosing project is missing a properties file, and that the file will be created if anything is written to it.

The following text is an example of a warning that might appear when you run any of the assembly lines that are contained in the qradar\_integration project that is included with IBM OpenPages with Watson:

```
Wed Aug 19 11:13:35 EDT 2015 [qradar_integration] WARN - CTGDIR103W
The properties file 'C:/SDI-Solutions/workspace/qradar_integration/Runtime-qradar_integration/
qradar_integration.properties'
for Properties.qradar_integration was not found, and will be created if anything is written to it.
```

These warnings can be safely ignored. In general, a Security Directory Integrator project typically has an associated properties file named after the enclosing project to hold any project-specific properties, but this file is not strictly required.

## Do not include security domain groups when creating object filters or security rule formulas

---

When creating filters for object types using the **Administration > Object Types** pages or security rule formulas that involve fields permitting user group selection, it is possible to select a security domain group because these groups are included in the selection list. The selection will not be flagged as an error. However, if you include a security domain group in the object filter criteria or in the security rule, you might encounter application errors later.

To avoid potential errors, ensure that you select a valid user group, and not a security domain group. In

the product user interface, security domain groups are represented by this icon  , and user groups are represented by this icon .

## Objects can be saved with an empty required field

---

If an object contains a redacted field that is also a required field, a user can successfully save the object even when the redacted field value is empty in the OpenPages repository.

## JSON file might not display multibyte characters correctly in Wordpad

---

When you export a JSON file for a Dashboard tab configuration and open it in Microsoft Wordpad, multibyte characters might be corrupted.

This issue might occur if you go to **Administration > Profiles**, select a Dashboard tab that uses multibyte characters, click **Edit** and then click **Export JSON**. If you select Wordpad as the application to open the file, the multibyte characters might not display correctly.

The solution is to open JSON files in a text editor that supports UTF-8. The JSON file will display correctly in Notepad or Microsoft Word.

## Remediating after an Enumerated String field is changed to a multi-select field (Db2)

---

If you are using IBM Db2, a subsequent maintenance task is required whenever you convert an enumerated string from single to multi-select. You do not need to do this task immediately. Do this task during your next available maintenance window.

### About this task

After an enumerated string field is changed to multi-select, the associated reporting schema tables in the OpenPages database will contain obsolete columns. The application handles the presence of these columns, but a subsequent cleanup should be scheduled in the next available maintenance window. If left unmanaged, these obsolete columns might eventually cause errors in OpenPages.

You can resolve the issue by running a utility against the Db2 database. Alternatively, you can drop and re-create the reporting schema to resolve the issue.

### Procedure

1. Log on to the OpenPages admin application server as a user with administrative privileges.
2. Stop all OpenPages services.
3. If you are using Microsoft Windows, start the Db2 command line processor by typing db2cmd.
4. Log in to CLPPLUS as the OpenPages database user, for example openpages.
5. Run the following command:

```
call OP_RPS_MGR.DROP_AND_REORG_OBSOLETE_RT_COLS;
```

The length of time that it takes for the command to run varies depending on the number of tables with obsolete columns that need to be dropped and the size of those tables.

When the command completes, the following message is displayed:

```
DB250000I: The command completed successfully.
```

## System delay when modifying object types and fields (Db2)

---

If you are using IBM Db2 and the reporting schema is enabled, you can encounter a significant system delay in OpenPages if you make object model modifications. The delay is due to locking conflicts on the IBM Db2 platform.

The following object model modifications can cause a system delay:

- Associating a field group to an object type
- Adding a new field to a field group that is already associated to an object type
- Converting a single valued enumerated field to a multi-valued enumerated field

- Adding new object type associations

To reduce a system delay, follow this process:

1. Choose a time when there is limited or no activity on the system.
2. Enable System Admin Mode.
3. Shut down IBM Cognos Analytics.
4. Disable global search.
5. Complete the object model modifications.
6. Start IBM Cognos Analytics.
7. Enable global search.

Object model modifications cause implicit DDL operations to be performed against the reporting schema.

On the IBM Db2 platform share locks are automatically acquired when a read operation is performed.

A read operation can block the object model modification. If the read operation is long running, for example, a long running Cognos report, the object model modification can appear to hang. In reality, the object model modification is not hanging but blocked on the session that is performing the read operation. After the read operation completes, the session that is attempting the object modification can proceed. The read operation needs to complete and clear its locks before the implicit DDL operation can acquire the locks that it needs to implement the object model change. If you kill the object model modification operation, the system can be left in an inconsistent state. If this happens, you must re-create the reporting schema.

The following actions do not cause this issue:

- Creating a new object type
- Creating a new field group
- Adding fields to a field group that is not yet associated to an object type
- Changing object text values
- Switching a field from not required to required or vice versa
- Changing the order of enumerated strings in an enumerated field
- Hiding an enumerated field value
- Adding new values to an existing enumerated field
- Modifying profile definitions
- Creating new reporting periods
- Enabling or disabling existing object type associations
- Enabling or disabling of security rules
- Enabling or disabling field level encryption

## NoClassDefFoundError errors when you run custom code

If you have custom deliverables, such as a JAR file or JSP, that uses third-party APIs, you might see a NoClassDefFoundError error. The error happens because Liberty does not enable third-party APIs by default. You need to enable access to third-party APIs.

To resolve the error, edit the apiTypeVisibility attribute in the <OP\_HOME>/wlp-usr/servers/<server\_name>Server<#/>/configDropins/overrides/op-apps.xml file. For example:

```
<classloader id="opappClassLoader" apiTypeVisibility="+third-party" commonLibraryRef="jaas-proxy" privateLibraryRef="ext-lib" />
```

For more information, see [Accessing third-party APIs from a Java EE application](#) in the Liberty documentation.

## Risk Assessment Summary report does not show related risks and controls

---

The **Risk Assessment Reports > Risk Assessment Summary** report does not show related risks and controls.

This issue can occur when you use the object relationship **Risk Assessment > Process > Risk > Control**.

To resolve the issue, update the reporting framework, and then regenerate the framework.

1. Click  > **System Configuration > Settings**.
2. Go to **Platform > Reporting Framework V6 > Models > Operational\_Risk\_and\_Control > Namespaces > RA1 > Object Model**.
3. In the **Value** field, replace RiskAssessment|SOXRisk with the following text:

```
RiskAssessment|SOXProcess,SOXProcess|SOXRisk
```

4. Click **Done**.
5. Regenerate the reporting framework for the **Operational Risk and Control** model.. For more information, see [“Updating the reporting framework” on page 817](#).
6. Open the Risk Assessment Summary report. The report now displays risks and controls that are associated with the risk assessment.

## Changing the settings for assessments in IBM OpenPages Operational Risk Management

---

If you haven't created any objects yet, you can change the settings for risk assessments. These settings are used by IBM OpenPages Operational Risk Management.

### About this task

When you install OpenPages, you specify the following settings for ORM: Module Assessment Method (qualitative or quantitative), Total Likelihood Count, and Total Impact Count.

You can change these settings later by running a script. The script updates a loader file, which you then import into OpenPages to re-configure ORM.

**Note:** If you've already created objects, you can run the script but any existing objects are not updated. You might need to do some manual remediation. The script is designed for fresh installations of ORM.

### Procedure

1. Set java\_home in `<OP_HOME>/Module/loaderdata/AssessmentMethodUpdate/post_install_update_ORM_assessment_settings.sh|.bat`.
2. Run the script:

#### Linux

```
cd <OP_HOME>/Module/loaderdata/AssessmentMethodUpdate
./post_install_update_ORM_assessment_settings.sh <likelihood_count> <impact_count>
<assessment_method_type>
```

#### Windows

```
cd <OP_HOME>\Module\loaderdata\AssessmentMethodUpdate
post_install_update_ORM_assessment_settings.bat <likelihood_count> <impact_count>
<assessment_method_type>
```

Where:

- `<likelihood_count>` is a value between 1 and 10

- <impact\_count> is a value between 1 and 10
- <assessment\_method\_type> is qualitative or quantitative

The script modifies the following loader file with the settings that you passed to the script: <OP\_HOME>/Module/loaderdataORM/AssessmentMethodUpdate\_PostInstall/ORM-assessment-settings-op-config.xml

3. Import the loader file into OpenPages. You can use ObjectManager or **Import Configuration**.

#### **ObjectManager**

Linux

```
./ObjectManager.sh l c OpenPagesAdministrator <password> <path_to_xml_file> ORM-assessment-settings
```

Windows

```
ObjectManager.cmd l c OpenPagesAdministrator <password> <path_to_xml_file> ORM-assessment-settings
```

For more information, see “[Load command example](#)” on page 734.

#### **Import Configuration**

Click  > **System Migration** > **Import Configuration**. Validate the <OP\_HOME>/Module/loaderdataORM/AssessmentMethodUpdate\_PostInstall/ORM-assessment-settings-op-config.xml file and then import it.

For more information, see “[Importing configuration items to the target environment](#)” on page 727.

4. Verify the changes.
  - a) Log in to OpenPages.
  - b) Click  > **Solution Configuration** > **Calculations**.
  - c) Verify that the calculation for the assessment type that you chose is enabled. For example, if you changed the assessment type to Qualitative, verify that **Qualitative Risk Rating** is enabled and **Quantitative Risk Rating** is disabled.
5. Update the deploy.properties files with the new values for ORM.
  - a) Open the <op\_installer>/src/deployment/<deployment\_name>/deploy.properties file in a text editor.
  - b) Update the following properties:

```
module_assessment_method =
module_likelihood_count =
module_impact_count =
```

## Troubleshooting helpers

If you encounter a problem with a helper, you can configure registry settings to create logs for the helper.

For more information, see the *Troubleshooting helpers* topic in the *IBM OpenPages with Watson Solutions Guide*.

## Users or group properties are overwritten in IBM OpenPages for IBM Cloud Pak for Data

In IBM OpenPages for IBM Cloud Pak for Data, if you set some user or group properties in OpenPages, you might find that they were overwritten.

In IBM OpenPages for IBM Cloud Pak for Data, you create and configure users and groups in Cloud Pak for Data and then they are synchronized to OpenPages.

Because users and groups are synchronized from IBM Cloud Pak for Data, if you change the following properties in OpenPages, your changes are overwritten when the synchronization job runs.

User properties

- User Name
- First Name
- Last Name
- Email
- Description
- All fields in Password and Security

Group properties

- Description

For more information about user and group synchronization in IBM OpenPages for IBM Cloud Pak for Data, see [How users and groups are synchronized from Cloud Pak for Data to OpenPages](#).

## OpenPages API documentation

---

For information about IBM OpenPages with Watson APIs, see the *IBM OpenPages with Watson Developer Guide*.



---

# Appendix D. Best practices for configuring IBM OpenPages with Watson

To improve the performance of IBM OpenPages with Watson, administrators can design, configure, and implement OpenPages with Watson applications using best practices. These suggested guidelines are provided to help you maximize, streamline, and get the most out of the product environment.

## Use short field names and field group names

---

When creating field groups and field names, use short field group names and short field names.

The length of field group names and field names have the following impacts:

- Long names restrict the number of fields that you can have on an object type.
- Long names increase the length of object type user defined attributes (UDAs), which have a 64 character maximum.

After creating the short field group names and short field names, an administrator can relabel and localize the field names to add meaning. For example, an administrator might create a field called AudDesEff, which can be difficult for a user to interpret. In the **Object Text** area of the application, the administrator can update the locale and change the label to a more meaningful name, such as Audit Design Effectiveness. By doing this, the administrator minimizes the length of the name but also retains a positive user experience.

## Limit the number of security rules and complexity of security rules

---

As an OpenPages administrator, you can use Field Level Security (FLS) and Record Level Security (RLS) in the IBM OpenPages with Watson application to create another level of robustness for implementing security.

You can use the rule engine to implement a variety of business security options. With this flexibility, remember that the more complex the rule, the more time it will take to evaluate the rule. The same is also true for the number of rules that are being implemented.

In other words, security rules and evaluating security rules adds a level of overhead to end user operations. End user operations include but are not limited to tasks such as updating an object, using the bulk update in a grid view, and filtering through data.

## Limit the number of SOXBusEntity objects in the system

---

The SOXBusEntity object type is a special object type. When an OpenPages power user or OpenPages administrator creates a SOXBusEntity object type in the IBM OpenPages with Watson application, an additional overhead is associated with it.

For example, it might create an additional security context point for OpenPages administrators. This creates additional administrative overhead for administrators. Additionally, adding additional SOXBusEntity object types also adds additional load to the security cache engine.

## Be aware of shared field groups

---

When using a field group that is shared among other object types, the administrator should be aware that a small change in that field group will have an effect on all the object types using it.

The IBM OpenPages with Watson application allows an object type to use multiple field groups. These field groups can also be used by other object types.

If an administrator adds one or two fields to the shared field group, those one or two fields will now also be associated with the object types that are using it. If one of the other object types is near the dynamic reporting schema SQL limitation of 32,000, it may cause problems regenerating the reporting schema.

## Eliminating unused object type relationships

---

If the business only requires a subset of the available enabled relationships, those unneeded relationships should be disabled.

### About this task

When you install the IBM OpenPages with Watson solutions, it loads dozens of object types and hundreds of parent-child relationships. Depending on your business needs, your business object model may only use a small subset of the object types and a subset of the parent-child relationships.

Disabling unused object types will prevent any accidental creations of those relationships.

With Oracle databases, one method of analyzing if there are any unused and enabled relationships is to run an SQL script. From the installation media, there are folders that contain SQL scripts. One of the SQL scripts within the folder is: Analyze-Object-Type-Relations.sql.

For IBM Db2 information, see the [IBM Db2 documentation](#).

### Procedure

1. Log on to SQL\*Plus as the OPENPAGES oracle id.
2. Type the following command to allow the output to occur: SET SERVEROUTPUT ON;.
3. Type the following to spool the contents to a log: SP00L AnalyzeRelationships.txt;.
4. Run the script by typing @Analyze-Object-Type-Relations.sql.
5. Run the following to stop the spooling of the log: SP00L OFF; .

The log file will identify any relationships that are enabled in the system but there are no instances of data utilizing those relationships.

## Task-oriented hyperlinking

---

You can add hyperlinks that are directly oriented to user tasks, from internal or external locations to IBM OpenPages with Watson views. These hyperlinks can also include filters.

For example, in a notification email to a risk owner, you can include a hyperlink to the grid view for Risks with the **Risks Awaiting Assessment** filter added to the link.

You can add hyperlinks to the following locations:

- OpenPages reports
- Notification emails
- OpenPages Java Server Page (.jsp) file type helper applications
- Within the OpenPages application, using computed fields or URL link fields

You can create hyperlinks that include the following target views:

- The task view for a specific object instance.
- The grid view for a specific object type.
- The creation view for a specific object type.

For some views, you can use parameters:

- For object types, use the object type name, not the label. See "Object name mapping" in the *IBM OpenPages with Watson Solutions Guide*.
- For filters, use the name of a public filter.

- For object instances, you need the `resourceId` of the instance. To find the `resourceId` of an object, open a task view. The `resourceId` is in the URL.

The following sample URLs can help you to create task-oriented hyperlinks:

### To a grid view for an object type

Syntax:

```
/openpages/app/jspview/react/grc/grid/<object type name>
```

Example: This link opens the grid view for Risks.

```
/openpages/app/jspview/react/grc/grid/SOXRisk
```

### To a grid view for an object type with a filter specified

Syntax:

```
/openpages/app/jspview/react/grc/grid/<object type name>
&view=Filtered%20List&filter=<public filter name>
```

Example: This link opens the grid view for Risks with the My Risks filter applied.

```
/openpages/app/jspview/react/grc/grid/SOXRisk?filter=My%20Risks
```

### To a task view

Syntax:

```
/openpages/app/jspview/react/grc/task-view/<object instance resourceId>
```

Example: This link opens the task view for an object instance with the resourceId 9048.

```
/openpages/app/jspview/react/grc/task-view/9048
```

### To a creation view with only the object type specified

Syntax:

```
/openpages/app/jspview/react/grc/creation-view/<object type name>
```

Examples: This link opens the creation view for Controls.

```
/openpages/app/jspview/react/grc/creation-view/SOXControl
```

### To a creation view with the object type and parent specified

Syntax:

```
/openpages/app/jspview/react/grc/creation-view/<object type name>
/initialParentId/<parent object id>/parentObjectType/<parent object type name>
```

Example: This link opens a creation view for a Control and sets the parent to a Risk with the resourceId 9229.

```
/openpages/app/jspview/react/grc/creation-view/SOXControl/initialParentId/9229/
parentObjectType/SOXRisk
```



# Appendix E. Creating custom actions for GRC workflows

You can create custom actions to use in IBM OpenPages with Watson workflows.

A custom action is a Java class that can be invoked during a workflow action. A custom action is very similar in function to a trigger, which executes on object operations. But triggers and custom actions have different interfaces and abstract implementations, so the classes are not interchangeable. Like triggers, custom actions must be deployed to each OpenPages application server and are dynamically loaded during startup.

To implement a custom action, do the following tasks:

- Create a custom action Java class by extending the abstract implementation `com.ibm.openpages.api.workflow.actions.AbstractCustomAction`
- Add the class to a JAR file. Use the JAR file for all of your custom code. Deploy the JAR file to each OpenPages application server in the `<OP_HOME>/aurora/op-ext-lib` directory.
- Restart the OpenPages application servers so that the custom action can be picked up by the dynamic class loader.
- Configure the custom action within the context of a workflow by using the **Custom Action** operation type. Set any property values or fields that the custom action requires as inputs.

Custom actions run in the order of operation that is listed in the workflow action.

All operations in a workflow action are performed in a single transaction. This means that if a custom action fails for any reason, the entire workflow action is rolled back.

## Passing arguments to a custom action

In order for the custom actions to be reusable in different contexts, properties and field values can be passed in during configuration. This is optional. As the developer of the custom action class, you decide which, if any, arguments to pass in and validate.

- Properties are name-value pairs that you define. For example, you might create a custom action that creates a child object and has a property that is named `object_type` that determines the type of object to create.
  - The custom action needs to validate that the properties that it expects to be passed in have been passed in and that they have valid values.
  - You can use expressions, such as `[$END_USER$]` or `[$TODAY$]` in the property values to pass in dynamic content. For a full list of expressions, see [“Using variables, functions, and fields” on page 377](#).
- Fields can also be passed in to provide a typed value to an object field. This technique can be very useful if your custom action is interacting with objects, either setting or evaluating field values.

## Authoring the custom action Java class

The only requirement of a custom action Java class is that it extends `com.ibm.openpages.api.workflow.actions.AbstractCustomAction`. This requirement is validated when the custom action is defined in a workflow.

A single abstract API must be implemented in `AbstractCustomAction`:

```
process();
```

Use this method to contain the business logic that the custom action will perform.

For more information about the IBM OpenPages GRC Java API, which you can use in custom actions, see *IBM OpenPages GRC Java API* in the *IBM OpenPages with Watson Developer Guide*.

You can access context about the current workflow and configuration through the following methods on `AbstractCustomAction`:

- `getContext()` – Returns an `IWFApplicationContext` object that contains all relevant information about the workflow state and the associated `GRCOobject`.
- `getPropertyValue(String prop_name)` – Returns the value of a named property.
- `getFields()` – Returns a `List<IWFFieldSetter>` object based on the configuration of the custom action.

Exception or validation messages can be thrown from a custom action and displayed to the user. To display messages, use:

```
throwException(String message, Throwable cause)
```

Use this method to throw exceptions and display a custom message to users. Uncaught exceptions or exceptions that are explicitly thrown are logged by the application, but only a general error message is displayed to users.

## Workflow context

The class `com.ibm.openpages.api.workflow.actions.IWFApplicationContext` provides state information for the workflow action.

Related workflow data:

- `IWFProcessDefinition getProcessDefinition()` – Returns the workflow definition.
- `IWFProcess getProcess()` – Returns the current workflow instance.
- `IWFActivityInstance getActivityInstance()` – Returns the current stage instance.
- `IWFTransition getTransition()` – Returns the current workflow action.

Related `GRCOobject`:

- `IGRCObject getResource()` – Returns the `GRCOobject` for the workflow instance.
- `Id getResourceId()` – Returns the ID of the `GRCOobject`.

Service API access:

- `IServiceFactory getServiceFactory()` – Returns a service factory for instantiating other OpenPages GRC API services.

## Tips

- Updating objects:

If you want your custom action to update an object for the current workflow action, access the object through `IWFApplicationContext.getResource()`. Updates that are made in this way are saved automatically by the workflow engine. Use this technique so that changes by multiple operations during an action are saved only once.

If your custom action looks up other objects and modifies them, the custom action must save the objects explicitly. You can save the changes by using `IResourceService.saveResource()`. For example, if your custom action updates controls that are children of a risk, save the controls explicitly.

- Utility functions:

The class `com.ibm.openpages.api.workflow.actions.util.WFActionUtil` has some useful utility functions that you can use in a custom action. Review the *IBM OpenPages with Watson API Javadoc* for a full list of functions.

Examples:

- `replaceStringExpressions(IWF0perationContext context, String value)` – This function takes any string value and replaces expressions in it. This function is very useful if you want to leverage expressions in property values that are passed in to your custom actions.
- `setFieldValue(IWF0perationContext context, IGRCObject grcObject, IWFFieldSetter field)` – This function updates the object with the field setter value that is passed in. This field can also use expressions in its value.



---

## **Appendix F. Personal information processed and stored by OpenPages**

IBM OpenPages with Watson stores certain personal information (PI). The personal information is stored in the OpenPages repository, specifically in the OpenPages database.

OpenPages stores and processes the following basic personal information:

- User name
- First name (given name)
- Last name (surname)
- Email address

For more information, see [Chapter 5, “Users, groups, and domains,” on page 39.](#)



# Appendix G. Legacy features

The following features have been deprecated or removed from IBM OpenPages with Watson.

## Legacy registry settings

The following registry settings are no longer used but might still appear in the system.

### Email registry settings

Some email-related registry settings are being deprecated. These settings will remain in the database in OpenPages 8.3 but will be removed in a future release. The settings have been replaced as indicated in the following table in order to use a single set of settings rather than multiple settings for different solutions.

<i>Table 256. Email settings</i>	
<b>Deprecated</b>	<b>Replaced with</b>
/OpenPages/Solutions/ORM/Email	/Applications/Common/Email
/OpenPages/Solutions/ORM/Email/From Name	/Applications/Common/Email/Mail From Name
/OpenPages/Solutions/ORM/Email/From Email	/Applications/Common/Email/Mail From Address
/OpenPages/Solutions/PCM/Attestation/Email Sender Name	/Applications/Common/Email/Mail From Name
/OpenPages/Solutions/PCM/Attestation/Email Sender Address	/Applications/Common/Email/Mail From Address
/OpenPages/Solutions/PCM/Publishing Policy/Email Sender Address	/Applications/Common/Email/Mail From Address
/OpenPages/Solutions/PCM/Publishing Policy/Email Sender Name	/Applications/Common/Email/Mail From Name
/Platform/Publishing/Mail/From Address	/Applications/Common/Email/Mail From Address
/Platform/Publishing/Mail/Host	/Applications/Common/Email/Mail Server
/Platform/Publishing/Mail/Transport Protocol	/Applications/Common/Email/SMTP Security Type
/Platform/Publishing/Mail/Username	/Applications/Common/Email/SMTP User Name

### Home Page settings

The Home Page settings are being deprecated. These settings will remain in the database in OpenPages for upgraded systems but will be removed in a future release.

These settings were used to globally configure the display of predefined tables, the number of embedded reports, the number of objects in a table, and the number of report listings. There were also settings for configured home page filtered lists that set the view definition that determines which fields were displayed, the target view of the Name hyperlink, and the target view of the View Details hyperlink.

- **Applications > GRCM > Home Page > Items**
- **Applications > GRCM > Home Page > <profile> > Items**
- **Applications > GRCM > Home Page > My Work Home Page Can Be Personalized**
- **Applications > GRCM > Home Page > Maximum Embedded Reports**

- Applications > GRCM > Home Page > Maximum Objects
- Applications > GRCM > Home Page > Maximum Reports Listing

## Other settings

The following settings are no longer used:

- Applications > GRCM > Filtered List > Filter on all fields in profile
- Applications > GRCM > Filtered List > Editable
- Applications > GRCM > Filtered List > Show All Objects
- Applications > GRCM > Filtered List > Filter on all fields in profile
- Applications > GRCM > Filtered List > Enable Object Type and Field Export Choices
- Applications > Common > Rich Text Editor > Third Party plugins > Enable CodeCogs(r) Equation Editor
- Applications > Common > Configuration > Use Legacy Associate
- Applications > Common > Configuration > Error Messages > Logging Level
- Applications > Common > Configuration > Copy Options > Max Object Trees Copied Interactive
- Applications > Common > Configuration > Copy Options > Max Top-level Objects Copied Interactive
- Applications > Common > Configuration > Copy Options > Show Copy Options Page
- Applications > Common > Configuration > Copy Options > Show Name Conflict Resolution Options
- Applications > Common > Configuration > Copy Options > Show Object Copy Options
- Applications > Common > Configuration > Copy Options > Use Legacy Copy
- Platform > Security > IE XSS Filter
- Applications > GRCM > Enable File Checkout
- Applications > GRCM > List View > Sort by Modification Date
- Common > Custom ACL Object Types
- Applications > Common > Administration > Users and Groups > Page Size
- Applications > GRCM > Auto Naming > Copied Object
- Platform > Repository > Resource > Move > Self-Contained Object Types > Legacy Move Behavior
- Applications > GRCM > Add New Wizard > Disable Add New Global Launch Point
- Applications > GRCM > Add New Wizard > Disable Add New Home Page Filtered List Global Launch Points
- Applications > GRCM > Detail Page > Use Actor Search Only
- Applications > GRCM > NavigationMenu > Administration > Schema > SpecialObjectTypes
- Applications > Common > Optimized File Upload
- Applications > GRCM > List View > Page Size
- Applications > GRCM > NavigationMenu > Administration > SubItems

## Legacy application permissions

---

The following permissions are no longer used but might still appear in the system.

### Administration permissions

The following Administration permissions are no longer used or the user interface to access them has changed.

*Table 257. Administration application permissions*

Permission	Description
Access Control Lists	Allows super administrators to view, edit, and remove the access control listings for objects.
Cognitive	Allows administrators to configure natural language classifiers in the Standard UI.
CompareEnvironments	Allows users and members of user groups to use the Compare Environments tool through the <b>Administration &gt; Compare Environments</b> menu item.

## **IBM CommandCenter Studio Cognos Analytics permission**

This application permission no longer enables the **Reporting > Cognos Analytics** menu item.

This application continues to allow users and members of user groups to access IBM Cognos Analytics from IBM OpenPages with Watson through the **Analytics** link in the primary menu.

## **Project Management permission**

If your system is configured to enable Project Management, this application permission allows users and members of user groups who are assigned role templates that include the permission to use the Milestone and Milestone Action Item Project Management capabilities.

## **Access permissions**

**Log in:** All users have access to the UI.

## **Browse Files permission**

This application permission allows users and members of user groups to view and go to the **Browse** menu item on the **My OpenPages > Attachments** menu in the Standard UI.

This permission applies to the Standard UI only.

## **Folders permission**

This application permission enables users and members of user groups to create new folders in the object repository that do not correspond to business entities. This allows users to create their own folder structure.

This permission applies to the Standard UI only.

## **Legacy FastMap import parameters**

The following parameters are no longer used but might still appear on the **Definition** tab of an exported workbook.

The following FastMap import parameters are no longer used.

*Table 258. FastMap import parameters*

Parameter	Description
<b>viewName</b> (no longer used)	<p>Specifies the view definition that is used by FastMap to validate fields. Any fields that are loaded that are not in this view are reported as invalid.</p> <p>The value can be set to the following values:</p> <ul style="list-style-type: none"><li>• The name of a Navigational View or Object View. The name is case-sensitive. Fields specified as read only are not imported.</li><li>• PROFILE_FIELDS. If the field is in the user's profile, it is imported, regardless of the view.</li></ul> <p>If the value is null or invalid, or if an object type is missing from the view, the Admin view is used to validate fields instead.</p>

## Notices

---

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service. This document may describe products, services, or features that are not included in the Program or license entitlement that you have purchased.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing  
IBM Corporation  
North Castle Drive  
Armonk, NY 10504-1785  
U.S.A.

For license inquiries regarding double-byte (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing  
Legal and Intellectual Property Law  
IBM Japan Ltd.  
19-21, Nihonbashi-Hakozakicho, Chuo-ku  
Tokyo 103-8510, Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation  
Location Code IE9  
Tower 3  
900 Chelmsford Street

Lowell, MA 01851-5114  
U.S.A.

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

If you are viewing this information softcopy, the photographs and color illustrations may not appear.

This Software Offering does not use cookies or other technologies to collect personally identifiable information.

## Copyright

---

Licensed Materials - Property of IBM Corporation.

© Copyright IBM Corporation, 2003, 2023.

US Government Users Restricted Rights – Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written.

These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. You may copy, modify, and distribute these sample programs in any form without payment to IBM for the purposes of developing, using, marketing, or distributing application programs conforming to IBM's application programming interfaces.

## Trademarks

---

IBM, the IBM logo and ibm.com are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at "[Copyright and trademark information](#)".

Adobe, the Adobe logo, PostScript, and the PostScript logo are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, and/or other countries.

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

The registered trademark Linux is used pursuant to a sublicense from the Linux Foundation, the exclusive licensee of Linus Torvalds, owner of the mark on a worldwide basis.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

Red Hat®, JBoss®, OpenShift®, Fedora®, Hibernate®, Ansible®, CloudForm, RHCA®, RHCE®, RHCSA®, Ceph®, and Gluster® are trademarks or registered trademarks of Red Hat, Inc. or its subsidiaries in the United States and other countries.

UNIX is a registered trademark of The Open Group in the United States and other countries.





# Glossary

---

In this glossary, you can find terms and definitions for IBM OpenPages with Watson

## **access control list (ACL)**

A concept in computer security used to determine the permissions (Read, Write, Delete, and Associate) a user or group can have on the folder structure of an object type (such as, an Entity, Risk, or Test). ACLs provide a means to control who has access to what and with which permissions. ACLs can be assigned to groups and users via a role template.

## **Action menu**

The menu that is displayed in views. To reveal menu items, hover your mouse pointer over a menu name. Your permissions determine which menus and items are available.

## **Actor ACLs**

These are a set of administrator access rights (Manage, Lock, Unlock, Reset Passwords, Assign Roles, Browse) defined on users and groups. These access rights control the operations an administrator can perform on a particular user or group.

## **administrator**

A user that is granted special permission to manage a Business Entity, including the assignment of Roles to users and groups.

## **application permissions**

A list of permissions that allow groups and users to access certain activities, including administration, within the application (such as the ability to view, lock, or unlock objects, or create and delete reporting periods).

## **associations**

Relationships that exist among objects, or between objects and attached files. Example: A sub-entity may be directly associated with a process or business function.

## **audit universe**

The aggregate of all areas within an organization that can be audited.

## **business unit**

One or more Entities, Processes or Sub-Processes.

## **CSV**

Comma separated values. A type of file that uses a comma-delimited format.

## **group**

A generic term that encompasses both organizational and security domain groups.

## **object**

Any item that contains or receives information, such as Business Entities, Processes, Risks, Controls, Issues, Tests and so forth. In a security context, an object is the piece of data to which access control is applied (such as, Business Entity, Process, Sub Process, Risk Assessment). Also called "resource".

## **object type**

A category or type of object, such as a Risks, Controls, Issues and so forth. In a hierarchy of objects, each object type has a set of allowed relationships with other object types.

## **organizational group**

A group that is created by an administrator to organize users within an organization. Organizational groups are typically associated with security domain groups and other organizational groups.

## **recursive object**

An object type that can have a parent object and child objects of its own type, potentially multiple layers deep. Examples of recursive object types include business entities, sub-accounts, sub-mandates, and sub-processes. For example, a business entity can have a parent business entity, such as Global Financial Services, and multiple child business entities, such as Compliance, Finance, HR, and IT, each of which can have child business entities.

**resource**

See "object".

**Resource ACLs**

These are a set of access rights (Read, Write, Delete and Associate) defined on the parent folder of an object. These access rights control the operations a user can perform on the folder and any objects under that folder.

**role**

An instance of a role template that is applied to a set of Users/Groups for a specific security context. Roles are granted to Users/Groups which allows them access to objects with certain permissions. Some examples of roles are: Process Owner, Control Owner, and Tester.

**Role template**

A security object that you can use to define all aspects of application security for various groups and users within a business unit. It contains access control definitions on folder structures for object types and application permissions. Role templates generally reflect the usual or expected function that a user or group plays within an organization. Some examples of Role templates that can be defined are Process Owner, Control Owner, and Tester. The template can then be applied to different Users/Groups for a specific security context.

**security context point**

A point defined in the OpenPages security model that you can use to assign roles to users and groups for controlling access and application permissions to objects under that security point.

**security domain group**

A group that is automatically created by the system when a business entity or subentity is created. Business entity security domain groups are located under the top level (root) **Security Domains** folder in the  > **Users and Security** > **Domains & Groups** task.

# Index

## Numerics

3DES [61](#), [64](#)

## A

acceptable use link  
    login screen [451](#)  
    menu item [476](#)

access control on Role groups  
    settings [501](#)

access controls  
    field level [92](#)  
    record level [87](#)  
    security rules [87](#), [92](#)

access logging [693](#)

accessibility for disabled [475](#)

ACL  
    permission values [74](#)  
    permissions [73](#)

add  
    keys to the Custom folder [455](#)  
    report [129](#)  
    role template [76](#)

adding  
    dependent fields in TFUI [212](#)  
    dependent pick lists [214](#)  
    field groups [160](#)  
    fields [161](#)  
    file types [203](#)

adding a custom field for search results [526](#)

adding business entity selector fields to views [289](#)

adding certificate snap-in

    Microsoft Internet Information Services [654](#)

adding Natural Language Classifier (object association suggestions) [309](#)

adding Natural Language Classifier (taxonomy suggestions) [288](#)

adding TLS binding  
    Microsoft Internet Information Services [656](#)

Admin View  
    associating objects [254](#)

Admin Views  
    adding a card layout [292](#)  
    adding a grid layout [304](#)  
    defining [271](#)

administering global search [517](#)

Administration menu  
    acceptable use [476](#)  
    privacy statement [476](#)

administrator  
    Super Administrator [41](#)  
    types of permissions [43](#)  
    user-provisioning permissions [43](#)

administrator permissions  
    assigning [45](#)  
    modifying [45](#)

administrator permissions (*continued*)  
    revoking [45](#)

AES [61](#), [64](#)

alert notification behavior [516](#)

allowed browsers [479](#)

Allowed Suspicious Character Combinations [513](#)

Apache configuration file  
    editing [660](#)

Apache load balancer server  
    certificate authority approval [662](#)  
    editing Apache configuration file [662](#)  
    generating a key pair and request [661](#)  
    importing the root certificate [662](#)  
    TLS configuration [661](#)

Apache web server  
    importing the root certificate [657](#)  
    importing the server certificate [658](#)

Apache Web Server  
    generating a key pair and request [656](#)  
    TLS configuration [656](#)

API settings  
    enable custom REST service setting [502](#)  
    paging [503](#)

application permissions

    Audit Trail [57](#)  
    Browse Files [964](#)  
    CommandCenter Studio [964](#)  
    CommandCenter Studios [57](#)  
    defining [51](#)  
    Folders [964](#)  
    Issues [57](#)  
    non-SOX [58](#)  
    Project Management [964](#)  
    setting on a group [52](#)  
    View Admin tab [58](#)  
    View Locks [58](#)

application readiness [711](#)

application server  
    default port [627](#)  
    Java and process management changes [688](#)  
    JDBC connection pools [688](#)  
    session management [688](#)  
    threadpool sizing [688](#)

application servers  
    starting Windows service [709](#)  
    stopping Windows service [711](#)

application text

    about [447](#)  
    folder categories [447](#)  
    modifying in the UI [449](#)  
    report keys [138](#)

application, starting [709](#)

applications folder settings [474](#)

Asian characters [443](#)

assigning  
    permissions [45](#)  
    roles to user or group [76](#)

associating  
group 51  
objects in Admin View 254  
profiles to ugroups 224  
profiles to users 224  
association heuristic (reassigning primary parents) 504  
asynchronous background jobs 547, 548, 579, 580  
audit  
Audit Change Report 125  
audit change values 125  
event 125  
filter settings 514  
Primary association 125  
audit configuration changes 634  
audit management events settings 514  
Audit Report 634  
aurora log file  
backing up 697  
maximum size 697  
aurora.properties file  
preparing passwords 63  
auroralogging.properties 697  
automatic restart 709

## B

back icon 475  
background jobs 547, 548, 579, 580  
background processes 547, 579  
backing up  
aurora log file 697  
backup utility  
OpenPages application server 548, 581  
overview 548, 581  
Backup utility  
refreshing a test environment 560  
Backup Utility  
.zip file 553, 586, 591  
about 545, 555, 577  
CommandCenter 552  
custom files 549, 583  
large files 553, 586, 591  
manifest file 549, 583  
OPBackup file formats 550, 586  
OPCCBackup file formats 553, 591  
OpenPages CommandCenter 588  
password encryption 581  
refreshing a test environment 558, 600  
running 550, 583  
running background jobs 547, 579  
running live backups 585  
running OPCCBackup 553, 559, 590  
storage 549, 586  
bandwidth, improve 685  
batch processing 767  
best practices  
deleting unused object types 954  
field groups 953  
field names 953  
limit complexity of security rules 953  
limit number of security rules 953  
limit number of SOXBusEntity objects in system 953  
security rules 102  
shared field groups 953

Boolean  
data type 155  
browser  
best practices 707  
locale settings 707  
security 706  
setting time out 704  
browser back and forward icons 475  
browser configuration  
Certificate Authority certificates 652  
browsers  
troubleshooting  
known problems and solutions 704  
bucket heading 449  
bulk move  
Allow Hierarchical Moves setting 497  
business entity selector fields  
adding to views 289

## C

CAF setting 706  
cascading signature settings 491  
certificate authority approval  
Apache load balancer server 662  
IBM HTTP 659, 664  
web server 655, 657  
Certificate Authority certificates 652  
certificate renewal 671  
certificate renewal on WebSphere 673  
Certificate Signing Request file 650  
certificates  
iKeyman tool 660, 664, 665  
importing 650  
importing into Java 652  
changing IP address for Oracle server 641  
child objects  
access controls 87  
more than the maximum number of associations 201  
security rules 95  
Codes  
Locale 443  
cognitive services  
configuring 852, 854–856  
Cognos  
services 717  
Cognos Application Firewall 706  
Cognos dispatcher service URL 505  
Cognos logout URL 505  
Cognos SDK URL 505  
Cognos TLS certificate renewal on Apache 673  
Cognos TLS certificate renewal on IIS 671  
colors  
in the UI 159  
command line  
Security Directory Integrator 826  
CommandCenter  
Backup Utility 552  
restore utility 592  
common folder settings 500  
compression  
see HTTP compression 685  
computed field definitions  
exporting 756

computed fields  
    creating 181  
    creating with multiple namespaces 185  
    defining 183  
    expression 182  
    importing 181  
    model an equation 182  
    nesting 185  
    report specification 182

configuration changes  
    migrating 719

configuration files  
    Apache load balancer server 662

Configuration Settings  
    modifying 473

configure  
    password requirements 60

configuring  
    password policies 60  
    security provider 62

Configuring cognitive services 850

configuring email notifications 820

configuring global search 523

configuring global search properties 538

configuring global search settings 527

configuring GRC Workflow 369

Configuring GRC Workflow 369

Configuring the reporting framework 799

Configuring the Scheduler 435

configuring the UI 229

Configuring Watson Assistant 843

Connection Refused error message  
    troubleshooting 827

connector currency values  
    specifying 824

connector date values  
    specifying 824

connectors 824

connectors,  
    overview 819

controller conditions  
    copying 212

cookieSecure 654

Copy Access From Inactive setting 480

Copy User Info Attributes setting 480

Copy User Info Choice setting 480

copying access from one user to another 50

creating  
    computed fields 181  
    long string index 611  
    long string index in Db2 568  
    organizational group 51  
    scheduled jobs to synchronize long string index 570, 613

creating a profile 220

creating public filters  
    object types 195, 198–200, 203, 204, 208, 954

Creation Views  
    adding a card layout 292  
    adding a classifier field that makes object association suggestions 309  
    adding a classifier field that makes taxonomy suggestions 288  
    adding a grid layout 304

Creation Views (*continued*)  
    adding actions to relationship fields 313  
    arranging fields in columns 280  
    defining 263  
    defining a Get Watson Classifier action 317  
    defining a New action 315  
    defining a Recursive Copy action 315  
    defining a Set Primary Parent action 314  
    defining an Add action 313  
    defining dynamic filters on relationship fields 317  
    designing 260  
    displaying a number field as a progress bar 287  
    displaying a URL field as a button or link 287

cross-context sharing 506

cross-site scripting  
    filter setting 511  
    Safe Tags setting 512

CSR file  
    generating 650

csv file  
    formatting 167  
    uploading 168

cultures 444

currency  
    data type 155

currency exchange rates  
    adding 167  
    currency exchange rates  
        disabling 168  
        editing 167, 168

currency field definitions  
    exporting 755  
    importing 754

Custom folder  
    adding new keys 455  
    using 455

custom indexes  
    re-creating 509

custom jobs  
    defining in the Scheduler 437  
    implementing a Java class 440  
    managing in the Scheduler 435  
    running in the Scheduler 435

custom settings  
    create 499  
    delete 499

customizing global search after initial enablement 525

customizing global search on initial enablement 524

CyberArk 646

## D

dashboard and story templates  
    modifying 137

Dashboard tab  
    troubleshooting JSON export 947

Dashboards  
    configuring in the UI 230

dashboards and stories  
    Cognos 135

data load template 776

data source 642

data types  
    Boolean 155

**data types (continued)**  
 currency 155  
 date 155  
 decimal 155  
 enumerated string 155  
 fragment 155  
 integer 155  
 long string 155  
 security rules 96  
 selecting 155  
 simple string 155

**database**  
 about online backups 593  
 changing references 641  
 crash recovery 600  
 Db2 back up and restore 555  
 disable online backup 600  
 online backup 592  
 Oracle 10g 641  
 RMAN 592

**database passwords**  
 updating 637

**database references, change** 641

**database server**  
 default port 627

**datapump** 577

**date**  
 data type 155

**date data types** 96

**dates function results** 503

**Db2**  
 back up and restore database 555  
 native encryption 677

**Db2 database**  
 tuning 689

**Db2 Text Search**  
 enabling for long string filtering 567

**decimal**  
 data type 155

**decrypting**  
 OpenPages repository 111

**Default Allowed Profiles setting** 481

**default profile** 221

**Default User Change Password setting** 481

**Default User Password Expiration setting** 481

**DefaultTemplate.xlsx** 785

**defining**  
 application permissions 51  
 field groups 160  
 Grid Views 257

**defining a theme** 243

**defining default filters for Grid Views** 286

**defining editable and read-only rules** 319

**defining Greater, GreaterEqual, Less, LessEqual, and Equal rules** 322

**defining MinLength and MaxLength rules** 323

**defining pattern rules** 324

**defining required rules in views** 321

**defining warnings in views** 324

**Definition worksheet**  
 parameters 784  
 unhide 784

**delegate activities**  
 administrator 41–43

**deleting**  
 dependent fields 211, 212  
 dependent picklists 214  
 filters 204, 205, 208, 566–568, 570, 571, 610–615  
 profiles 222  
 rules 102

**deletion interval for reporting period** 479

**dependent field**  
 adding in TFUI 212  
 modifying controllers 212

**dependent fields**  
 copying controller fields 212  
 deleting 102, 208, 212, 214, 222

**dependent picklists**  
 adding 214  
 configure 214  
 deleting 214  
 enabling or disabling 214  
 modifying 214

**deployments** 719

**designing**  
 Grid Views 256

**designing a Creation View** 260

**development deployment** 719

**disabling**  
 field level encryption keystore 111  
 profiles 219–223, 495

**disabling associations between**  
 object types 195, 198–200, 203, 204, 208, 954

**disassociating**  
 group 51  
 profiles from groups 225  
 profiles from users 225

**display name format** 450

**domains** 39

**dropping**  
 long string index 571, 614

**dynamic fields** 211

**E**

**editing**  
 profiles 219–223, 495

**editing properties**  
 object types 195, 198–200, 203, 204, 208, 954

**email**  
 configure Notification Manager 925  
 configure OPBackup notification 545, 578

**email notifications**  
 configuring 820  
 customizing for GRC Calculations 366  
 customizing for GRC Workflow 432

**enable associations of child objects** 493

**enable custom REST service setting** 502

**enabling**  
 currency exchange 753  
 field level encryption keystore 111  
 OpenPages repository 111  
 profiles 219–223, 495

**enabling and disabling**  
 field dependency behavior 212

**enabling associations between**  
 object types 195, 198–200, 203, 204, 208, 954

**enabling file attachment search** 522

enabling file types for search [522](#)  
enabling global search [521](#)  
enabling or disabling  
  dependent picklists [214](#)  
enabling or disabling object types or fields for global search  
[523](#)  
encryption  
  db2 [677](#)  
  field level [110](#)  
  password [106](#)  
encryption algorithm  
  change AES key [65](#)  
  legacy systems [64](#)  
  UPEA tool [61](#)  
encryption key  
  algorithm [105](#)  
  changing AES [65](#)  
encryption keystore  
  editing [111](#)  
Entity Move/Rename Utility  
  about [572, 622](#)  
  input file [574, 623](#)  
  run as a scheduled task [576, 626](#)  
  run interactively [575](#)  
enumerated string  
  data type [155](#)  
environment files  
  password encryption [581](#)  
environment migration  
  best practices [725](#)  
  dependent items migrated [722](#)  
  exporting items [727](#)  
  importing items [727](#)  
  items migrated [720](#)  
  items not migrated [722](#)  
  process of [726](#)  
  settings [485, 719](#)  
  validating the import [727](#)  
equations  
  modeling [182](#)  
Excel worksheet. See FastMap. [771](#)  
excluding fields  
  object type [226–228](#)  
excluding from a profile  
  object type [226–228](#)  
excluding object types  
  profile [224–226](#)  
excluding settings from migrating [762](#)  
export  
  disable for object types [495](#)  
exporting  
  computed field definitions [756](#)  
  configuration data [719](#)  
  currency field definitions [755](#)  
  data [731](#)  
  workflow definitions [241, 432](#)  
exporting and importing dashboards [241](#)  
exporting configuration changes [763](#)  
exporting data [763](#)  
exporting metadata changes  
  ObjectManager [731, 735, 762, 934](#)  
expressions for GRC Calculations  
  functions for currency values [359](#)  
  functions for dates [357](#)

expressions for GRC Calculations (*continued*)  
  functions for lists and numerical values [354](#)  
  functions for string values [353](#)  
  If/then/endif statements [360](#)  
  syntax rules [344](#)  
  testing and debugging [365](#)  
  tutorial [347](#)  
  using system variables [352](#)  
EXTEND rule [81](#)  
external system, import data [793](#)

## F

fallback profile [221](#)  
FAQs  
  global search [542](#)  
FastMap  
  access [770](#)  
  define the path of an object [777](#)  
  Definition worksheet [783](#)  
  errors and warnings [771](#)  
  export data into template [776](#)  
  export settings [495](#)  
  export template [784, 785](#)  
  import process [768](#)  
  locale [769](#)  
  optimize performance [795, 796](#)  
  overview [767](#)  
  parameters [784, 786](#)  
  securing import templates [796](#)  
  template [768](#)  
  user profile [769](#)  
  validation [769](#)  
  validation messages [772](#)  
  worksheet [768](#)  
FastMap import parameters [965](#)  
field dependency behavior  
  enabling and disabling [212](#)  
field groups  
  adding fields to [161](#)  
  adding to object types [160](#)  
  best practices [953](#)  
  best practices for shared [953](#)  
  defining [160](#)  
field guidance [477](#)  
field level encryption  
  disabling the keystore [111](#)  
  enabling the keystore [111](#)  
  key [105](#)  
  keystore [105](#)  
field level security  
  redaction  
    field level security [93](#)  
  security  
    field level [94](#)  
field names  
  best practices [953](#)  
fields  
  applying colors to value ranges [158](#)  
  decrypting  
    fields [164](#)  
  encrypting  
    field values [163](#)  
  encrypting values for [163](#)

fields (*continued*)  
  excluded 216  
  including in an object type 227  
  long string  
    encrypting 163  
  simple string  
    encrypting 163  
  system workflow fields 376  
fields from an object type  
  excluding 226, 228  
file attachment search  
  enabling 522  
  enabling file types 522  
file type information  
  configuring 202  
file types  
  adding 203  
  associating with object types 203  
filters  
  adding to object types 208  
  associating views 208  
  considerations before you begin 205  
  copying 208  
  creating Db2 long string index 568  
  creating long string index 611  
  creating scheduled jobs to synchronize long string indexes 570, 613  
  deleting 102, 208, 212, 214, 222  
  dropping long string indexes 571, 614  
  enabling DB2 Text Search for long strings 567  
  enabling Oracle Text for long strings 612  
  modifying 208  
  stop words for long string indexes 615  
  utilities for long strings 566, 610  
Fix Central 939  
fragment  
  data type 155

## G

general elements in the View Designer 278  
generating a CSR  
  iKeyman tool 659, 663  
generating a key pair and request  
  Apache Web Server 656  
generating a keystore and key pair  
  IBM HTTP Server 658, 663  
global search  
  add a custom field 526  
  administering 517  
  configuring 523  
  customizing after initial enablement 525  
  customizing on initial enablement 524  
  enabling 521  
  enabling or disabling object types or fields 523  
  OPBackup and OPRestore 520  
  properties 538  
  re-creating index 522  
  settings 527  
  starting services 712  
  stopping services 713  
  unhiding settings 527  
global search FAQs 542  
global search properties

global search properties (*continued*)  
  error handling parameters for the indexer 538  
  maximum file attachment text for indexing 541  
  maximum heap size 539  
  maximum opsearchtool.jar heap size during indexing 539  
  maximum Solr heap size 539  
  maximum text extraction heap size during indexing 540  
  root path location for file attachment search 541  
  setting the text extractor timeout limit 540  
globalization 444  
GRC Calculations  
  building expressions 342  
  calculate on object save 327  
  calculation definitions 328, 337  
  cascade effect 333  
  configuring 327  
  customizing email notifications 366  
  defining 338  
  designing 333  
  FAQs 330  
  functions for currency values 359  
  functions for dates 357  
  functions for lists and numerical values 354  
  functions for string values 353  
  how to delete a calculation 337  
  how to disable a calculation 337  
  how to publish a calculation 337  
  how to save a calculation 337  
  If/then/endif statements 360  
  permissions 327  
  running as administrator 364  
  syntax rules for expressions 344  
  system variables 352  
  testing and debugging 365  
  tutorial for writing expressions 347  
  use cases 336  
GRC Workflow  
  assignees 372  
  configuring 369  
  customizing email notifications 432  
  defining a standard stage 397  
  defining a start stage 397  
  defining a workflow 391  
  defining an end stage 402  
  defining applicability for a workflow 392  
  defining assignees for a stage 397  
  defining autostart or manual start for a workflow 392  
  defining criticality for a workflow 392  
  defining overall due date for a workflow 392  
  defining oversight users for a workflow 392  
  defining stage due dates 397  
  defining stage properties 397, 402  
  defining subscribers for a stage 397  
  defining task view overrides for a stage 397  
  defining workflow properties 392  
  designing a workflow 379  
  due dates 379  
  enabling and disabling a workflow 392  
  exporting and importing workflow definitions 432  
  fundamental concepts 370  
  GRC Workflow Designer 382  
  how to start a workflow 373  
  how users interact with workflows 373

GRC Workflow (*continued*)  
    implementing a Java class 957  
    inserting fields, URLs, and application text 377  
    inserting variables 377  
    managing workflow instances 431  
    oversight users 372  
    participants 372  
    permissions 369  
    running reports that include workflow information 434  
    stage due dates 379  
    starting workflow instances in bulk 430  
    subscribers 372  
    system workflow fields 376  
    workflow definitions 370  
    workflow due date 379  
    workflow instances 370

GRC Workflow Designer  
    how to use the keyboard 385

grid views 495

Grid Views  
    defining 257  
    defining default filters for Grid Views 286  
    designing 256  
    displaying a number field as a progress bar 287

group  
    OPAdministrators 39

groups  
    associating 51  
    associating profiles 224  
    creating 51  
    disassociating 51  
    disassociating profiles 225

gzip format 550, 553, 586, 591

## H

hidden settings 479

Home page  
    in the UI 230

host setting 505

hostname, database server 641

HTTP  
    security 511

HTTP compression  
    about 685  
    disabling 685

http\_access.log 693

httpd.conf file  
    editing 660

httpSession 654

hyperlinking  
    to views 954

## I

IBM Cognos service  
    starting and stopping 717  
    starting and stopping on Linux 718  
    starting and stopping on Windows 717

IBM HTTP Server  
    certificate authority approval 659, 664  
    generating a keystore and key pair 658, 663  
    TLS configuration 663

IBM OpenPages  
    restore 545

IBM OpenPages application and database  
    backup 545, 577  
    Db2 back up and restore 555  
    restore 545, 577

IBM OpenPages CommandCenter  
    backup 545  
    Db2 back up and restore 555

IBM OpenPages SDI Connector for UCF Common Controls

Hub 824

IBM Watson Language Translator 498

IIS 685

iKeyman tool  
    generating a CSR 659, 663  
    importing certificates 660, 664, 665

import data  
    external system 793  
    see also FastMap 767

importing  
    configuration data 719  
    currency field definitions 754  
    data 731  
    workflow definitions 241, 432

importing changes 765

importing configurations 765

importing root certificate  
    Microsoft Internet Information Services 655

importing the server certificate  
    Apache web server 658

indexes  
    adding 507  
    example 508

inline guidance  
    adding to views 280

installation  
    default ports 627

instance name, database 641

integer  
    data type 155

interactive reports 438

interactive task  
    Entity Move/Rename Utility 575

IP address  
    static 641

IT governance 881

## J

Java  
    importing certificates 652

Java and process management changes  
    application server 688

Java classes  
    implementing for custom jobs 440  
    implementing for GRC Workflow 957

java.security file 62

JDBC connection pools  
    application server 688

JDBC data source 642

JSON  
    arranging fields in columns 280  
    inline guidance 280  
    Task View header 284

JSON (*continued*)  
  tips for editing 277  
JSON export  
  troubleshooting 947  
JSON tips for editing 277  
JSP report jobs  
  defining in the Scheduler 438

## K

key pair and request  
  Apache load balancer server 661  
  Microsoft Internet Information Services 654  
keys 455  
keystore  
  Db2 636  
  WebSphere Liberty 636  
keywords  
  security rules  
    field level 96  
    record level 96

## L

languages 444  
LDAP  
  authentication module, configuring 113  
  configuring for user accounts 47  
  mixed-mode authentication 115  
  user authentication 113  
Linux load balancer server  
  TLS configuration 658  
live backup 585  
loading  
  data 731  
locale browser settings 707  
Locale codes 443  
localizing  
  system fields 447  
lock and signature settings 490  
lock menu for display settings 492  
lock menu settings 493  
locked  
  parent object 493  
locking a user account 510  
locks  
  enabling and disabling 491  
  objects 492  
log files  
  access logging 693  
  OPBackup 550, 583  
  OPCCBackup 553, 590  
  OPCCRestore 554, 592  
  OPRestore 588  
login screen  
  messages 451  
long string  
  data type 155  
long string fields  
  running string concatenation 616  
  string concatenation SQL file 617  
  String Concatenation Utility 616  
long string indexes

long string indexes (*continued*)  
  creating 611  
  creating in Db2 568  
  creating scheduled jobs to synchronize 570, 613  
  dropping 571, 614  
  enabling Db2 Text Search 567  
  enabling Oracle Text 612  
  stop words 615  
  utilities 566, 610  
loss event entry  
  configuring 839  
  confirmation emails 837  
  designing the app pages 833  
  how dates are validated 835  
  how to launch 835  
  how users are handled 833  
  planning the configuration 831  
  where loss events get created 833  
  who gets assigned 834  
LTPA token 654

## M

mail server address  
  setting 486  
managing for object types  
  filters 204, 205, 208, 566–568, 570, 571, 610–615  
managing object types 195  
menus  
  modifying the order of 482  
messaging information 693  
Microsoft Internet Information Services  
  adding certificate snap-in 654  
  adding TLS binding 656  
  importing root certificate 655  
  key pair and request 654  
migrating  
  data 731  
migrating configuration changes 760  
migration  
  configuration changes 719  
missing Administration menu items  
  troubleshooting 942  
mode setting 491  
models, adding using the template model 810  
models, reporting framework 799  
modify  
  role template 77  
modify menu items 482  
modify settings 473  
modify text displayed in the UI 449  
modifying  
  controllers for dependent field 212  
  stop words for long string indexes 615  
  user accounts 49  
move entities  
  Entity Move/Rename Utility 572, 622  
  Entity Move/Rename Utility input file 574, 623  
multi-deployment environments 760  
multiple security context points 71

## N

namespace  
definition 800  
overview 800  
relational 814  
namespaces 812  
Namespaces and models, configuring 810  
Natural Language Classifier  
adding a classifier field that makes object association suggestions 309  
adding a classifier field that makes taxonomy suggestions 288  
Natural Language Understanding  
configuring 853  
New  
availability of object types 213  
configuring 213  
disable 478  
new features in version 8.2.0 27  
new features in version 8.2.0.1 24  
new features in version 8.2.0.2 22  
new features in version 8.2.0.3 20  
new features in version 8.2.0.4 19  
new features in version 8.3.0 14  
new features in version 8.3.0.1 13  
new features in version 8.3.0.2 12  
new features in version 9.0.0.0 9  
New User Default Locale setting 481  
Notification Manager  
properties 934  
numeric data types 96

## O

object aspect 125  
object fields  
identifying new 153  
Schema Analysis report 193  
setting a default value for 164  
threshold limit 193  
Object Manager tool 761  
object model diagrams  
viewing in the solution schema visualization editor 196  
object models  
viewing in the solution schema visualization editor 195  
object reset  
performing 468  
ruleset parameters 468  
session details 470  
session log 470  
starting 469  
status 470  
object resets  
currency fields 460  
overview 457  
preparing data 460  
system fields 460  
object text 445  
object type  
including fields 227  
including in a profile 226  
object type definitions  
accessing 198

object type profiles  
editing 198, 199, 222  
object types  
adding filters 208  
associating with file types 203  
deleting unused 954  
managing 195  
platform 195  
object types from a profile  
excluding 226, 228  
ObjectManager  
batch loader sample 735  
batch loader syntax 735  
loader files 731  
properties 934  
ObjectManager examples  
assigning or revoking role assignments 739  
creating or loading users 741  
importing file attachments 756, 757  
moving objects 736  
renaming objects 737  
ObjectManager tool 731  
objects  
associating in Admin View 254  
auto-naming settings 483  
locking and unlocking 492  
path expressions 95  
SOXDocument auto-naming settings 485  
online backup  
database 592  
op-backup-restore.env file  
preparing passwords 63  
OP-CUSTOM 64  
OPAdministrators 39  
OPBackup  
backup utility 548, 581  
configuring email 545, 578  
configuring gzip 550, 586, 591  
refreshing a test environment 558, 560, 600  
running 550, 583  
running live backups 585  
OPCCBackup  
about 588  
configuring email 545, 578  
configuring gzip 553  
running 553, 559, 590  
OpenPages CommandCenter  
Backup Utility 588  
restore utility 554  
running the Backup Utility 553, 559, 590  
OpenPages repository  
decrypting 111  
enabling 111  
encrypting 111  
OpenPages solutions  
FCM 1  
IAM 1  
ITG 1  
ORM 1  
PCM 1  
operators  
security rules 96  
OPRestore  
log files 588

Oracle  
     backing up databases [584](#)  
 Oracle Admin Client [577](#)  
 Oracle Data Pump  
     overview [577](#)  
 Oracle Enterprise Manager [641](#)  
 Oracle Instant Client [577](#)  
 Oracle server  
     IP address [641](#)  
 Oracle Text  
     enabling for long string filtering [612](#)  
 organizational group [51](#)  
 overwritten user and group properties  
     troubleshooting [950](#)

**P**

paging [503](#)  
 Palettes  
     in themes [241](#)  
 parameters  
     FastMap import [965](#)  
 parent object [493](#)  
 parent objects  
     access controls [87](#)  
     security rules [95](#)  
 password  
     change Oracle Native Driver password [608](#)  
     change Oracle password [638](#)  
     configure [60](#)  
     encryption algorithm [106](#)  
     modify encryption [61](#)  
     policies [60](#)  
 password encryption  
     keystore [105](#)  
 passwords  
     changing encryption algorithms [64](#)  
     changing in User table [63](#)  
     preparing for reencryption [63](#)  
 path expressions  
     objects [95](#)  
 paths  
     children [95](#)  
     parents [95](#)  
 permissions  
     application [52, 964](#)  
     assigning [45](#)  
     Audit Trail [57](#)  
     Browse Files [964](#)  
     CommandCenter Studio [964](#)  
     CommandCenter Studios [57](#)  
     define [51](#)  
     Folders [964](#)  
     GRC Calculations [327](#)  
     GRC Workflow [369](#)  
     Issues [57](#)  
     modifying [45](#)  
     non-SOX [58](#)  
     other application [58](#)  
     Project Management [964](#)  
     revoking [45](#)  
     setting for a group [52](#)  
     UI [229](#)  
     View Admin tab [58](#)

permissions (*continued*)  
     View Locks [58](#)  
 phonebook [449](#)  
 phonebook bucket size [482](#)  
 picklists  
     dependent [214](#)  
     modifying dependency behavior [214](#)  
 planning  
     views [255](#)  
 Platform folder settings [502](#)  
 platform object types [195](#)  
 Platform Reporting Framework folder settings [507](#)  
 Platform Reporting Schema folder settings [507](#)  
 Platform Security folder settings [509](#)  
 ports  
     default [627](#)  
     fixed [627](#)  
     virtual hosts [650](#)  
 postinstallation tasks  
     updating reporting schema [121](#)  
 Preference Objects  
     and GRC Workflow [379](#)  
 primary menu  
     modify menu order [482](#)  
 primary parent ID  
     specifying [821](#)  
 privacy link  
     login screen [451](#)  
     menu item [476](#)  
 privacy statement  
     login screen [451](#)  
 problem determination  
     exchanging information with IBM Support [940, 941](#)  
 production deployment [719](#)  
 profile  
     associating groups [224](#)  
     associating users [224](#)  
     disassociating groups [225](#)  
     disassociating users [225](#)  
     including object types [226](#)  
 profiles  
     creating [220](#)  
     default [221](#)  
     deleting [222](#)  
     disabling [111, 223](#)  
     editing [198, 199, 222](#)  
     enabling [111, 222, 753](#)  
     fallback [221](#)  
     guidelines [219](#)  
     prevent from exporting [495](#)  
 properties and parameters  
     aurora.properties [931](#)  
     server properties [933](#)  
     sosa properties [934](#)  
     tools properties [934](#)  
 Properties and parameters [931](#)  
 properties file  
     HTTPS address [665](#)  
     TLS port [665](#)  
 properties files  
     editing for TLS [653](#)  
 property bundles  
     creating [161](#)  
 provisioning users [47](#)

publish reports 129  
publishing reports  
    limitations 139  
    server user interface 135

## Q

QRadar integration package  
    troubleshooting  
        known problems and solutions 946  
QRadar integration project  
    using 820  
Questionnaire assessments  
    configuring 829

## R

RapidRatings 921  
RCM 893, 919  
RCM Theme Deployer 915  
record level security  
    security  
        record level 81, 85  
recursive object types  
    defining levels 802  
    rules 803  
Redirect Template 129  
redirect the security log off link 510  
reencryption  
    password 63  
regenerate  
    reporting framework 814  
    reporting schema 117  
    Reporting schema  
        accessing 117  
Registry settings, apply to all models 806  
Relationship fields  
    adding a card layout 292  
    adding a chart diagram 294  
    adding a count 303  
    adding a grid layout 304  
    adding a tree diagram 307  
    adding actions to 313  
    defining a Delete action 317  
    defining a Get Watson Classifier action 317  
    defining a New action 315  
    defining a Recursive Copy action 315  
    defining a Set Primary Parent action 314  
    defining an Add action 313  
    defining dynamic filters on 317  
rename  
    Allow Hierarchical Moves setting 497  
rename entities  
    Entity Move/Rename Utility 572, 622  
    Entity Move/Rename Utility input file 574, 623  
report fragments  
    settings 485  
reporting fragment fields  
    defining 178  
    fields requiring parameter information 179  
    limitations 176  
    name 179  
    object ID prompt 180

reporting fragment fields (*continued*)  
    planning considerations 177  
    report path 179  
    reporting period ID prompt 181  
    tasks to configure 177  
reporting framework  
    generating 814  
    object types 809  
    permissions 816  
    planning the configuration 806  
    regenerate 814  
    understanding 799  
reporting framework, models 799  
reporting period  
    ACLS 457  
    application permissions 458  
    change history 457  
    creating 458  
    delete 459  
    deletion period setting 458  
    disable 459  
    overview 457  
    reporting schema 457  
    system administration mode 458  
reporting schema  
    adding indexes 507  
    creating and re-creating 120  
    enabling and disabling 120  
    re-creating custom indexes 509  
    updating 121  
    viewing 120  
Reporting schema  
    Administering 117  
    index example 508  
    permissions 119  
    Populating past reporting periods 119  
    relation to reporting period 119  
reporting server  
    default port 627  
    Tomcat heap size 689  
reporting service  
    tuning 689  
reports  
    Administrative Reports folder 125  
    Audit Reports folder 125  
    creating interactive 139  
    GRC Workflow 434  
    Issue Reports folder 125  
    managing 125  
    parameters 134  
    platform reports 125  
    running interactive 140  
    Schema Analysis report 193  
    supplied 125  
    top-level 125  
    understanding 130  
Reports  
    Issue 128  
    Security 128  
Reports Access Page Size setting 481  
required fields  
    setting in a profile 228  
    setting in the field definition 162  
    troubleshooting 946

resets, *See* object resets  
 restore IBM OpenPages database [551](#)  
 restore OpenPages database [587](#)  
 restore utilities  
     CommandCenter [591](#)  
     OpenPages CommandCenter [554](#)  
**Restore Utility**  
     about [545, 555, 577](#)  
     IBM OpenPages [587](#)  
     log files [588](#)  
     running [551, 587](#)  
**RESTRICT rule** [81](#)  
**revoking**  
     role from user or group [77, 79](#)  
**RiskLens** [881](#)  
**RiskRecon** [922](#)  
**RMAN** [592](#)  
**role**  
     assigning to user or group [76](#)  
     revoking from user or group [79](#)  
**role template**  
     create [76](#)  
     delete [77](#)  
     disabling [77](#)  
     enabling [77](#)  
     modify [77](#)  
     revoking from user or group [77](#)  
     view or modify [75](#)  
**role-based security model** [67](#)  
**root certificate**  
     Apache load balancer [662](#)  
     Apache web server [657](#)  
**rule analysis** [102](#)  
**rules**  
     editable and read-only rules [319](#)  
     Greater, GreaterEqual, Less, LessEqual, and Equal rules [322](#)  
     MinLength and MaxLength rules [323](#)  
     pattern rules [324](#)  
     required rules [321](#)  
     *See also* security rules  
**rules in views**  
     defining [318](#)  
**ruleset**  
     creating [461](#)  
     exporting XML file [471](#)  
     file, creating [461](#)  
     loading [468](#)  
     overview [457](#)  
     parameters [468](#)  
     sample [461](#)  
     tag library [463–467](#)

**S**

**safe** [646](#)  
**SAM**  
     enabling and disabling [37](#)  
**scenarios**  
     access to issue action items [90](#)  
     all users can view objects, some users can update objects [92](#)  
     exception management [92](#)  
     objects shared across GRC domains [89](#)

**scenarios (continued)**  
     privacy incidents [92](#)  
     security by function [91](#)  
**scheduled task**  
     Entity Move/Rename Utility [576, 626](#)  
**Scheduler**  
     configuring [435](#)  
     defining a custom job [437](#)  
     how to delete a custom job [435](#)  
     how to disable a job [435](#)  
     how to run a job [435](#)  
     kinds of jobs [435](#)  
     running JSP reports [438](#)  
**scheduling the Security Directory Integrator** [826](#)  
**schema**  
     reporting [121](#)  
     *See also* reporting schema  
**SDI** [824](#)  
**SDI connectors** [819](#)  
**SDI error messages**  
     troubleshooting [946](#)  
**search filter**  
     using advanced logic [210](#)  
**security**  
     advanced XSS filter setting [511](#)  
     Allowed Suspicious Character Combinations setting [513](#)  
     context point [68, 69](#)  
     cross-site scripting filter setting [511](#)  
     domain groups [72](#)  
     extending security context [70](#)  
     field level [92](#)  
     model [67](#)  
     model with multiple points [71](#)  
     Safe Tags setting [512](#)  
     triangle relationship [71](#)  
**Security Directory Integrator**  
     command line tips [826](#)  
     scheduling [826](#)  
     techniques [826](#)  
**security domains** [72](#)  
**security model**  
     Security Domains folder [72](#)  
**security provider**  
     configuring [62](#)  
**security rules**  
     access controls [87, 92](#)  
     best practices for [102](#)  
     best practices for limiting [953](#)  
     child objects [95](#)  
     data types [96](#)  
     deleting [102](#)  
     disabling [101](#)  
     enabling [101](#)  
     exporting [719, 731](#)  
     field level [95](#)  
     grammar [98](#)  
     importing [719, 731](#)  
     keywords [96](#)  
     operators [96](#)  
     parent objects [95](#)  
     paths [95](#)  
     record level [95](#)  
     reporting periods [457](#)  
     rulesets [457, 461](#)

security rules (*continued*)  
    scenarios 89–92  
    validating 102  
security, browser 706  
SecurityScorecard 919  
self-contained object type  
    about 501  
server properties and parameters 933  
services  
    Cognos 717  
    starting 709  
    starting and stopping Cognos service 718  
    starting and stopping IBM Cognos service 717  
    stopping 711  
session cookies 654  
session management  
    application server 688  
session timeout 704  
set  
    application permissions on a group 52  
settings  
    access control on Role groups 501  
    access the Settings page 473  
    accessibility 475  
    additional fields in search results 534  
    alert notification behavior 516  
    allow compression 535  
    Allow Hierarchical Moves 497  
    allow URL redirects 535  
    allowed browsers 479  
    Allowed Suspicious Character Combinations 513  
    Apache Solr password 537  
    Apache Solr user ID 537  
    applications folder 474  
    association heuristic (reassigning primary parents) 504  
    audit management events 514  
    auto-naming objects 483  
    browser cache 475  
    cascading signatures 491  
    child and parent 493  
    Cognos 505  
    common folder 500  
    Copy Access From Inactive 480  
    Copy User Info Attributes 480  
    Copy User Info Choice 480  
    copying folders 499  
    create custom 499  
    cross-context sharing 506  
    cross-site scripting filter 511  
    date field display format 487  
    Default Allowed Profiles 481  
    default number of search results to return per page 537  
    Default User Change Password 481  
    Default User Password Expiration 481  
    delete custom 499  
    deletion interval for reporting period 479  
    disable Add New 478  
    disable bulk update 496  
    editing for TLS 653  
    enable associations of child objects 493  
    enable create and delete custom settings 498  
    Enable custom REST service setting 502  
    environment migration 485, 719  
    Export Disabled Object Types 495  
settings (*continued*)  
    format of object names 483  
    grid view  
        export to Excel 495  
    host setting 505  
    illegal characters 500  
    internal page size for search results 533  
    language analyzer used by search 530  
    localization 503  
    localization settings 503  
    lock 490  
    lock and unlock objects 492  
    lock menu 493  
    lock menu for display 492  
    locking a user account 510  
    mail server address 486  
    Maximum Import Rows 500  
    Maximum Import Rows setting 500  
    Maximum Page Size 500  
    menus 482  
    modify menu order 482  
    network connection request timeout 535  
    New User Default Locale 481  
    number of allowed connections 536  
    number of allowed connections per host 536  
    number of attempts to fill the search results 533  
    number of records inserted per batch 532  
    number of records to cache 529, 530  
    number of request attempts 536  
    number of search results records cached per user session 533  
    object reset ACL restrictions 494  
    object reset locking restrictions 494  
    object reset logging level 494  
    object reset on error behavior 494  
    object resets 494  
    object types  
        number of levels to export 497  
    object types to exclude from bulk update 496  
    paging 503  
    path to global search administration server 528  
    path to server for search indexing 528  
    phonebook bucket size 482  
    Platform folder 502  
    Platform Reporting Framework folder 507  
    Platform Reporting Schema folder 507  
    Platform Security folder 509  
    polling interval 529  
    profiles to prevent from bulk updating 496  
    progress refresh interval 528  
    query path to the Apache Solr server 530  
    query path to the Apache Solr server for Folder ACL indexing 531  
    query path to the Apache Solr server that handles Folder ACL search requests 532  
    report fragments 485  
    reporting framework  
        adding namespaces 812  
        object types 809  
    reporting framework namespaces 812  
    Reports Access Page Size 481  
    security log off link 510  
    security safe tags 512  
    show field guidance 477

settings (*continued*)  
    show hidden 479  
    show system generated field guidance 478  
    signature 490  
    signature locks 491  
    signatures 490  
        socket timeout for indexing 536  
        socket timeout for searching 537  
    SOXDocument auto-naming objects 485  
    system security model 500  
        time to search before timing out 534  
    triangle object relationships 801, 808  
    URL of the Apache Solr server for Folder ACL indexing 531  
    URL of the Apache Solr server for search requests 534  
    URL path to the Apache Solr server for search requests 532  
    User Preferences folder 515  
    user provisioning 480  
    Users Can Copy Access From 481  
    view 495

Settings  
    modifying 473

settings)  
    object types to exclude in export 496

signature and lock settings 490

signature links for sign off 490

simple string  
    data type 155

solution schema visualization editor  
    about 195  
    using 196

solution schema visualizations  
    creating 197

sosa properties and parameters 934

SOXBusEntity objects  
    best practices for limiting 953

specifying a primary parent ID 821

specifying connector currency values 824

specifying connector date values 824

SSL, *See* TLS

SSL certificate  
    Cloud Pak for Data 874

ssoRequiresSSL 654

starting and stopping  
    IBM Cognos service 717, 718

static IP address 641

storage backup  
    enable and disable 549, 586

storage location  
    OPBackup 582

String Concatenation Utility  
    about 616  
    running 616  
    SQL file 617

string data types 96

sub-groups  
    removing 51

Super Administrator 41

Supply Wisdom 920

suspicious character combinations 513

System Admin Mode  
    enabling and disabling 37

system fields  
    system fields (*continued*)  
        localizing 447

system file management  
    adding and modifying files 150  
    assigning access control to folders 148  
    checking in files 150  
    checking out files 150  
    copying files and folders 148  
    creating folders 148  
    deleting files and folders 148  
    downloading files 150  
    managing 148  
    moving files and folders 148  
    opening files and folders in a Quick View 148  
    overview 145  
    refreshing trigger configurations 151  
    renaming files 148  
    uploading files 148  
    uploading modified files 150

system generated field guidance 478

system notice  
    login screen 451

## T

Task View header  
    adding to views 284

Task Views  
    adding a card layout 292  
    adding a chart diagram 294  
    adding a classifier field that makes object association suggestions 309  
    adding a classifier field that makes taxonomy suggestions 288  
    adding a count 303  
    adding a grid layout 304  
    adding a header 284  
    adding a tree diagram 307  
    adding actions to relationship fields 313  
    arranging fields in columns 280  
    defining 268  
    defining a Delete action 317  
    defining a Get Watson Classifier action 317  
    defining a New action 315  
    defining a Recursive Copy action 315  
    defining a Set Primary Parent action 314  
    defining an Add action 313  
    defining dynamic filters on relationship fields 317  
    designing 265  
    designing to use with GRC Workflow 379  
    displaying a number field as a progress bar 287  
    displaying a URL field as a button or link 287

task-oriented hyperlinking 954

techniques for Security Directory Integrator 826

template models, using in the reporting framework 810

test deployment 719

test environment  
    refreshing from production data 558, 560, 600

text  
    application 447  
    object 445

Theme Deployer 915

themes 241

Themes

- Themes (*continued*)
  - defining 243
  - system and custom 241
- Third Party Risk Management
  - RapidRatings 921
  - RiskRecon 922
  - SecurityScorecard 919
  - Supply Wisdom 920
- threadpool sizing
  - application server 688
- time-out period, browser 704
- TLS
  - accessing the OpenPages application 650
  - Apache load balancer server configuration 661, 662
  - Apache Web Server configuration 656–658
  - certificate renewal 671
  - Cognos 665
    - Cognos certificate renewal on Apache Web Server 673
    - Cognos certificate renewal on IIS 671
  - configuration 650
    - IBM HTTP Server 663
    - IBM HTTP Server configuration 658–660, 663–665
    - LDAP configuration 46
    - Linux load balancer server configuration 658
    - Microsoft IIS configuration 654–657
    - properties files configuration 665
    - WebSphere certificate renewal 673
    - WebSphere configuration 650, 652, 653, 874
  - Tomcat heap size
    - reporting server 689
  - tools properties 934
  - track configuration changes 634
  - triangle relationships 71
- troubleshooting
  - contacting IBM Support 939
  - exchanging information with IBM Support 940, 941
  - Export JSON 947
  - fixes
    - installing 939
    - getting fixes 939
  - identifying problems and techniques 937
  - known problems for browsers 704
  - known problems for the QRadar integration package 946
  - missing Administration menu items 942
  - overwritten user and group properties 950
  - required fields 946
  - SDI error messages 946
  - searching knowledge bases 938
  - security domains included in search 946
  - subscribing to Support notifications 941
- troubleshooting the Connection Refused error message 827
- tuning
  - Db2 database 689
  - reporting service 689
- U**
- UAT deployment 719
- UCF 824
- UI
  - configuring 229
  - Dashboards 230
  - defining a Creation View 263
- UI (*continued*)
  - defining a dashboard for a profile 230
  - defining a Task View 268
  - defining an Admin View 271
  - defining rules in views 318
  - designing a Task View 265
  - permissions 229
  - supported field value colors 159
  - system views 247
  - URL and URL redirects 229
  - using the View Designer 272
  - views 247
  - update data using FastMap 767
  - UPEA tool
    - syntax 63
  - uploading large files 487
  - URL for application
    - shortening 683
    - UI 229
  - user accounts
    - configuring LDAP access for 47
    - copying access 50
    - modifying 49
  - user administration 40
  - user guidance
    - adding to views 282
  - user names
    - exclude characters from 500
  - User Preferences folder settings 515
  - user provisioning
    - Copy Access From Inactive 480
    - Copy User Info Attributes 480
    - Copy User Info Choice 480
    - Default Allowed Profiles 481
    - Default User Change Password 481
    - Default User Password Expiration 481
    - New User Default Locale 481
    - Reports Access Page Size 481
    - Users Can Copy Access From 481
  - user provisioning settings 480
  - user-defined keys 455
  - username format 450
  - users
    - associating profiles 224
    - disassociating profiles 225
  - Users Can Copy Access From setting 481
  - users table
    - updating to change passwords 63
  - using advanced logic in a search filter 210
  - using OPBackup and Op Restore with global search 520
  - using the QRadar integration project 820
  - utilities
    - about backup and restore 545, 555, 577
    - CommandCenter Backup 552
    - CommandCenter Restore 591
    - Entity Move/Rename 572, 622
    - Entity Move/Rename input file 574, 623
    - filtering on long string indexes 566, 610
    - OPBackup 548, 581
    - OpenPages CommandCenter Backup 588
    - OpenPages CommandCenter Restore 554
    - OPRestore 551, 587
    - running OPBackup 550, 583
    - running OPBackup live 585

utilities (*continued*)  
running OPCCBackup 553, 559, [590](#)  
running OPCCRestore 554, [592](#)  
running OPRestore 551, [587](#)  
running string concatenation [616](#)  
String Concatenation [616](#)  
string concatenation SQL file [617](#)

## V

validating  
rules [102](#)  
validation rules  
defining warnings [324](#)  
vault [646](#)  
verify  
encryption algorithm [61](#)  
View Designer  
adding a card layout [292](#)  
adding a chart diagram [294](#)  
adding a count [303](#)  
adding a grid layout [304](#)  
adding a tree diagram [307](#)  
adding actions to relationship fields [313](#)  
defining a Delete action [317](#)  
defining a Get Watson Classifier action [317](#)  
defining a New action [315](#)  
defining a Recursive Copy action [315](#)  
defining a Set Primary Parent action [314](#)  
defining an Add action [313](#)  
defining default filters for Grid Views [286](#)  
defining dynamic filters on relationship fields [317](#)  
displaying a number field as a progress bar [287](#)  
displaying a URL field as a button or link [287](#)  
supported field value colors [159](#)  
user guidance [282](#)  
using [272](#)  
View Designer)  
adding a classifier field that makes object association  
suggestions [309](#)  
adding a classifier field that makes taxonomy  
suggestions [288](#)  
general elements [278](#)  
view settings [495](#)  
views  
planning [255](#)

## W

Watson Knowledge Catalog [874](#)  
web server  
certificate authority approval [655, 657](#)  
webAppSecurity [654](#)  
WebSphere  
configuring certificates [874](#)  
generating the CSR file [650](#)  
importing certificate into Java [652](#)  
importing certificates [650](#)  
TLS configuration [653](#)  
TLS ports on virtual hosts [650](#)  
what's new [9](#)  
Windows services  
starting [709](#)

Windows services (*continued*)  
stopping [711](#)  
workbook. See FastMap. [768](#)

## X

XSS  
cross-site scripting filter setting [511](#)  
Safe Tags setting [512](#)



**IBM.**<sup>®</sup>